

Version 3.6

Part No. 311643-C Rev 00
April 2001

600 Technology Park Drive
Billerica, MA 01821-4130

Reference for the Contivity VPN Switch

NORTEL
NETWORKS™

Copyright © 2001 Nortel Networks

All rights reserved. April 2001.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks NA Inc.

Trademarks

Nortel Networks, the Nortel Networks logo, and Contivity are trademarks of Nortel Networks.

Microsoft, Windows, and MS-DOS are trademarks of Microsoft Corporation.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

Java is a trademark of Sun Microsystems.

Firewall-1 is a trademark of Check Point Software Technologies, Ltd.

SecurID and ACE Server are trademarks of RSA Security Inc.

NDS is a trademark of Novell Inc.

Cisco and Cisco Systems are trademarks of Cisco Technology, Inc.

Entrust is a trademark of Entrust Technologies, Inc.

VeriSign is a trademark of VeriSign Incorporated.

OPENVIEW is a trademark of Hewlett-Packard Company.

NETVIEW is a trademark of International Business Machines Corp (IBM).

SPECTRUM is a trademark of Cabletron Systems, Inc.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks NA Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks NA Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed

by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks NA Inc. software license agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as “Software” in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH NORTEL NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License grant. Nortel Networks NA Inc. (“Nortel Networks”) grants the end user of the Software (“Licensee”) a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Nortel Networks Agent software or other Nortel Networks software products. Nortel Networks Agent software or other Nortel Networks software products are licensed for use under the terms of the applicable Nortel Networks NA Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Nortel Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Nortel Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Nortel Networks’ and its licensors’ confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Nortel Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee’s facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Nortel Networks warrants each item of Software, as delivered by Nortel Networks and properly installed and operated on Nortel Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Nortel Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Nortel Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Nortel Networks will replace defective media at no charge if it is returned to Nortel Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee’s intended results and for the installation, use, and results obtained from

the Software. Nortel Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Nortel Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Nortel Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL NORTEL NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF NORTEL NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO NORTEL NETWORKS FOR THE SOFTWARE LICENSE.

5. Government licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Nortel Networks of any such intended examination of the Software and may procure support and assistance from Nortel Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Nortel Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Nortel Networks copyright; those restrictions relating to use and disclosure of Nortel Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Nortel Networks the Software, user manuals, and all copies. Nortel Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Nortel Networks, 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN NORTEL NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST NORTEL NETWORKS UNLESS NORTEL NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Preface	49
Before you begin	49
Text conventions	49
Related publications	51
Hard-copy technical manuals	52
How to get help	52
 Chapter 1	
System	55
System Identity	55
System Identity	56
Management IP Address	56
Changing IP Addresses	57
Domain Identity	57
DNS Host Name	57
DNS Domain Name	57
DNS Server Address	57
Primary	57
Secondary	58
Tertiary	58
LAN Interfaces	58
LAN/WAN IP Addressing	59
Interface	60
Description	60
State	60
Enabled	60
Disabled	60
Type	60
Public	60
Private	61
Actions	61
Configure	61

Statistics	61
Edit	61
Delete	61
IP Address	61
Subnet Mask	62
Interface Filter	62
Edit LAN Interface	62
Interface	64
Speed/Duplex	64
Description	65
State	65
Interface Type	65
Add IP Address and Edit IP Address	66
Interface	67
IP Address	67
Subnet Mask	68
Interface Filter	68
Routing Information Protocol (RIP)	68
Enabled	69
Transmit	69
Receive	69
Authentication	70
Import Default Route	70
Poison Reverse	70
Export Default Routes Metric	70
Export Static Routes Metric	70
Export Branch Office Static Routes Metric	71
LAN Interface Statistics screen	71
Interface	75
IP Address	75
Description (Optional)	76
Interface Filter	76
State	76
Enable	76
Disable	76

Actions	76
Configure	76
Enable/Disable	77
Statistics	77
WAN Statistics	77
Configure WAN Interface Settings	80
Interface	81
Description (Optional)	81
Interface IP Address	82
Remote IP Address	82
Accept Negotiated Address	82
Specify Remote Address	82
Interface Filter	82
PPP Authentication Settings	83
PPP Advanced Settings	83
CSU/DSU Settings	83
T-1 with Integrated CSU/DSU	83
T1-CSU/DSU - LMC 1200	85
Clock Source	85
Line Build Out (dB)	86
Line Coding	86
HDLC Polarity	86
Line Framing	86
Performance Report Mesg	87
Fractional T-1	87
Local Authentication	87
None	88
PAP	88
CHAP	89
WAN Interface Advanced Settings	89
LCP Settings	90
Address Control Field Compression	90
Protocol Field Compression	91
Echo Fault Threshold	91
Echo Interval	91

IPCP Settings	91
VJ Negotiation	91
VJ Connect ID Compression Negotiation	92
VJ Max Slots	92
LCP/NCP	92
Interface Debug	92
IPX (Internetwork Packet Exchange)	92
IPX Configuration	92
Public Network Address	93
Default Nearest Server	94
Maximum SAP Entries	94
Maximum Route Entries	94
Private LAN Interfaces	95
Interface	95
Enable	95
Network Address	95
Frame Type	95
Hardware Encryption Accelerator	96
Bulk Accelerator	98
Auto Recovery Enabled	98
Description	99
Operational Status	99
Administrative States	99
Protocols	99
Algorithms	99
Crypto Strength	100
Boots	100
Uptime	100
Context Memory Size	100
Max Sessions	100
POST Results	100
Statistics	101
Date and Time	101
Date	102
Time	102

Day	102
Time Zone	103
Configure Network Time Protocol (NTP)	103
Servers	104
Server IP Address	104
Interface	104
Key ID	104
Bursting	104
Version	105
Actions	105
Trusted Keys	105
Key ID	105
Actions	106
Certificates screen	106
Key Usage Extensions Required	106
Enable Allow All Feature	107
Trusted	107
Type	108
Allow All	108
Subject DN (Distinguished Name)	108
Validity	108
Actions	108
Delete	108
Details	108
Import Tunnel Certificate	109
Generate Certificate Request	109
Import SSL Certificate	109
Create New Key and Certificate Request	109
Create New Key and Certificate Request	110
Common Name	110
Organizational Unit	110
Organization	110
Locality	111
State/Province	111
Country	111

Public Key Size	111
PKCS #10-Encoded Certificate Request	111
Paste PKCS #7 Base-64 Certificate	112
Server Certificate	113
Trusted CA Certificate	113
Pasting a PKCS #7 Certificate	114
OK	114
Certificate Details	114
This Certificate Belongs To	115
This Certificate Was Issued By	115
Validity Dates	116
Certificate Fingerprint	116
Default Group	116
Association of Certificate Subject DN with groups	116
Certificate Revocation List	116
Enabled	116
Search Base	117
Host	117
Connection	117
Status	117
Update Frequency	117
Switch Settings	118
Safe Mode Configuration	118
Enable Safe Mode	119
Safe Mode Duration	119
Serial Port Configuration	119
Menu Access Level	119
Mode	119
Baud Rate	121
Modem Initialization	121
Reset Serial Port	121
Log File Configuration	121
Log File Life Time	121
Forwarding	122
Proxy ARP for	122

Tunnel to Tunnel Traffic	123
Allow End User to End User	123
Allow End User to Branch Office	123
Allow Branch Office to Branch Office	123
.....	123
Chapter 2	
Services	125
Available Services	125
Allowed Services	126
Tunnel Types	127
Management Protocols	127
Authentication Protocols	128
Authentication	131
User Name and Password/Pre-Shared Key	131
RSA Digital Signature	131
RADIUS Authentication	131
Encryption	131
Types of Integrity Checks	133
Encapsulating Security Payload (ESP)	133
Authentication Header (AH)	134
IKE Encryption and Diffie-Helman Group	134
Authentication Order	134
Order	134
Server	135
Type	135
Associated Group	135
Action	136
Load Balance	136
Management IP Address	136
Fail-Over	136
Public IP Address	136
PPTP Settings	137
Authentication	138
Authentication Order	138

L2TP Settings	138
Authentication	139
Authentication Order	140
L2TP Access Concentrators	140
L2TP Add or Edit Access Concentrators	140
LAC/Switch	141
LAC/Switch UIDs	141
Secret	141
Confirm Secrets	141
L2F Settings	142
Authentication	143
Authentication Order	144
Network Access Servers	144
NAS/Switch UIDs	144
Names/Passwords	144
Action	144
L2F Add or Edit Network Access Server	145
NAS/Switch	145
RADIUS Service	146
Enable RADIUS Service	147
Port	148
Clients	148
Enabled	148
Host Name or IP Address	148
Secret	149
Confirm Secret	149
Action	149
Add RADIUS Service Client	149
Host Name or IP Address	150
Secret	150
Confirm Secret	151
Firewall/NAT	151
Configuration	152
Enabled	152
Firewall/NAT Type	153

Firewall/NAT Policy	154
Actions	155
Anti-Spoofing Configuration	156
Anti-Spoofing Enabled	156
Public Interface	156
IP Address	156
Edit Contivity Firewall	156
Connection Number	156
Logging	157
Contivity Tunnel Filter	158
Check Point FireWall-1 Service	158
Check Point FireWall-1 Start Up	160
Start Check Point FireWall-1 upon reboot	160
Check Point FireWall-1 Status	160
State	160
Condition	161
Check Point FireWall-1 Management Station	161
Host Name or IP Address	161
Shared Secret	162
Confirm Shared Secret	162
Check Point FireWall-1 Logging Hosts	162
Enabled	162
Host Name or IP Address	162
Shared Secret	162
Confirm Shared Secret	163
Backup	163
SysLog (System Forwarding)	163
Enabled	164
Host Name or IP Address	164
Message Level	164
Urgent	165
Normal	165
Detailed	165
All	165
Change System Logging Capture Level	165

Chapter 3**Routing 167**

Static Routes 167

Static Routes 168

Default Routes 168

Type 169

Gateway Address 169

Interface 169

Admin State 169

Cost 169

Action 169

Edit 170

Delete 170

Add Public Route 170

Add Private Route 171

Static Routes through Physical Interfaces 172

IP Address 172

Subnet Mask 173

Gateway Address 173

Interface 173

Admin State 173

Cost 173

Action 173

Edit 173

Delete 174

Add Route 174

Admin state 175

Cost 175

Network address 175

Subnet mask 176

Gateway address 176

Show Branch Office Routes 176

IP address 177

Subnet mask 177

Interface address 177

Gateway address	177
Admin State	177
Cost	177
OSPF	177
OSPF Configuration	178
Enabled	179
Router ID	180
AS-Boundary-Router	180
Known OSPF Areas	180
Area ID	180
Add	180
Edit	181
Area Range	181
Add an Area Range	182
Configured Physical Interfaces	182
IP address	182
Area ID	182
Type	182
State	182
Status	182
OSPF LSDB	182
Neighbor	184
Interfaces	185
Summary	186
Statistics	187
RIP	188
Enabled	189
Update Timer	189
Configured Interfaces	189
IP Address	189
State	190
Status	190
Statistics	190
Database	191
Interfaces	192

Interfaces	193
Physical interface	194
Protocol name	194
State	194
Actions	194
OSPF	195
Interface	195
IP Address	195
State	195
Area ID	196
Type	196
Authentication	196
Cost	196
Priority	196
Hello Interval	196
Dead Interval	196
Poll Interval	197
Retransmission Interval	197
Transmission Delay	197
RIP	197
Enabled	198
Transmit Mode	198
Receive Mode	199
Authentication	199
Poison Reverse	199
Import Default Route	199
Export Default Routes Metric	199
Export Static Routes Metric	200
Export OSPF Routes Metric	200
Export Branch Office Static Routes Metric	200
VRRP	200
Configured State	201
Master Status	201
Current Backed Up Addresses	202
New Backed Up Address	202

VRRP	203
VRRP Configuration	203
VRRP Screen	204
Addresses Configured for VRRP	205
Edit	206
Delete	206
Create	206
Create/Edit VRRP IP Address Screen	206
VRID	207
Advertise Interval	207
Authentication Type	207
Master Delay Mode	208
Status	210
Configuration	210
Errors	213
Route Table	214
Search For	215
Interface	216
Protocol	216
Save Route Table	216
Status	216
IP Forward Table	216
Route Table	218
Access List	219
Create	220
Current Rules for Access List: xxx	221
Edit	221
Delete	222
Move selected rule to position	222
New Rule	223
Action	223
Subnet	223
Mask	223
Mask Type	223
Policy	223

Route Policy Service	224
Redistribution Table	224
Protocol	224
Route Source	225
Policy List	225
Access Name/Number	225
Protocol	225
Interface	225
Policy Type	225
Action	225
Add	226
Client address redistribution	227
Client address redistribution	228
Enabled	228
Number of UTunnel Host Routes	229
Summarization	229
Status	229
Show User Tunnel Routes	229
Statistics	230
Status	231
OSPF LSDB	232
OSPF Neighbor	232
OSPF Interfaces	233
OSPF Summary	233
OSPF Statistics	233
RIP Database	233
RIP Interfaces	233
RIP Statistics	233
VRRP Config	233
VRRP Errors	233
VRRP Statistics	234
Route Table	234
Next Hop Table	234
Best Route Table	234
RTM Statistics	234

IP Forward Table	234
Chapter 4	
QoS (Quality of Service)	235
Classifiers	235
Current Multi-Field (MF) Classifiers	236
Create	236
Delete	236
Edit	237
Rules in Classifier	237
Available Rules	237
<< (Add Rule)	237
>> (Remove Rule)	237
Manage Rules	237
Current Rules	238
Create	238
Edit	238
Copy	238
Delete	239
Edit/Create Rules screen	239
Classifier Rule for	239
Source Address and Destination Address	239
Protocol	240
TCP/UDP Source and Destination Ports	241
Current DSCP Value	241
DiffServ Marking	241
QoS Interfaces	242
Current Interface	242
Bandwidth Management	243
Configure	243
DiffServ Edge	244
Multi-Field Classifier	245
Traffic Conditioning	246
EF Shaping	246
Traffic Conditioning Meter Settings	246

Egress (Outbound) Queueing Mode	247
Queueing Mode	247
Interface QoS Statistics	247
Bandwidth Management	248
Bandwidth Management	249
Admission Control	249
Bandwidth Rates	249
Current Bandwidth Rates	250
Delete	250
Create	250

Chapter 5

Profiles 251

Groups	251
Maximum Number of Logins	252
Groups screen	252
Group	253
Actions	253
Add Group screen	254
Inherited Attributes	254
New Attributes	254
Group Name	255
Parent Group	255
Edit a Group	256
Initial Configuration	256
Configure	256
Current Configuration	256
Connectivity Settings	257
Contact Information	258
Access Hours	259
Call Admission Priority	259
Forwarding Priority	259
Number of Logins	260
Password Management	260
Maximum Password Age	260

Minimum Password Length	260
Alpha-numeric Passwords	261
Static Addresses	261
Idle Timeout	261
Filters	262
IPX	262
Maximum Number PPP Links	262
RSVP	262
RSVP: Token Bucket Depth	262
RSVP: Token Bucket Rate	263
Address Pool Name	263
User Bandwidth Policy	263
IPSec Settings	264
Split Tunneling	265
Split Tunnel Networks	266
Client Selection	266
Authentication	267
Encryption	269
IKE Encryption and Diffie-Hellman Group	270
Perfect Forward Secrecy	270
Forced Logoff	270
Client Auto Connect	271
Banner	272
Display Banner	272
Client Screen Saver Password Required	272
Client Screen Saver Activation Time	272
Client Fail-Over Tuning	273
Allow Password Storage on Client	273
Compression	273
Rekey Timeout	274
Rekey Data Count	274
Domain Name	274
Primary DNS	274
Secondary DNS	274
Primary WINS	274

Secondary WINS	275
Nortel Client Requirements	275
Client Policy	275
Allow IPSec Data Protection	275
PPTP	276
L2TP	277
L2TP/IPSec Data Protection	277
Require IPSec Transport Mode Connections	277
L2F	278
Common Tunnel Settings	280
Authentication	280
Compression	281
Use Client-Specified Address	281
Common DNS and WINS Server Fields	282
Primary DNS	282
Secondary DNS	282
Primary WINS	282
Secondary WINS	283
User Management	283
Group	284
Display	284
Last/First	284
Actions	285
Add User	285
Search	285
User Add or Edit	286
Name	288
Group	288
Remote User	288
User Accounts	290
Expires (Days)	291
IPSec Certificate Credentials	292
Administration Privileges	293
Admin Rights	294
Filters	295

Current Filters	296
Edit	296
Delete	296
Create	296
Copy Filter	296
Edit Filter	298
Filter Set	298
Rules in Set	298
Allow Management Traffic	299
Manage Rules	302
Create	302
Edit	302
Copy	303
Delete	303
Creating, Editing, and Copying a Filters Rule	303
Rule Name or Filter Rule For:	305
Filter Action	305
Permit	306
Deny	306
Direction	306
Inbound	306
Outbound	306
Address	306
Protocol	307
Source and Destination Ports	307
TCP Connection	308
Established	308
Don't Care	308
Common Filter Modify Fields	309
Create	309
Edit	309
Delete	309
Current Addresses	309
Current Addresses	310
Create or Edit Address	311

Address Name	311
Address	311
Wildcard	312
Current Protocols	312
Current Protocols	313
Create or Edit Protocol	313
Protocol	314
Protocol Number	314
Current Ports	314
Current Ports	315
Create or Edit Port	315
Port Name	316
Port Number	316
Hours	317
Name	318
Edit	318
Delete	318
New Access Hours	318
Add	318
Edit Hours of Access	318
Day	319
Hours Allowed	319
Networks	320
Current Networks	320
Edit	321
Delete	321
Create	321
Networks Edit screen	321
Current Subnets For	322
New Subnets For	322
Domains	323
Current Domain Sets	324
Edit	324
Delete	324
Create Domain	324

Edit Domains screen	324
Current Domains in domain_set	325
New Domain for domain_set	325
Network Address Translation (NAT)	326
Creating NAT Sets	326
Translation Type	326
Internal	326
Start Address	326
End Address	327
External	327
Start Address	327
End Address	327
Branch Office	327
Edit	328
Delete	328
Test	329
Configure IP	329
Enable/Disable	329
Define Branch Office Connection	329
Add Group Button	330
Add Group screen	330
Edit Group	330
Configure IP	331
Connection Information	332
Routing	333
Static Routes	333
OSPF	333
RIP	334
Define Branch Office Connection	334
Connection Name	335
Group Name	335
Control Tunnel	336
Define Connection/Edit Connection	336
Connection Information	336
Connection Name	336

Group Name	336
State	336
Configure Routing	337
Configuration	337
Enable Branch Office Connection	337
Address	337
Accessible Networks	338
NAT	338
Filters	338
Tunnel Type	339
Authentication	339
IPSec Authentication	339
Pre-Shared Key: Text or Hex String	339
Certificates	339
PPTP Authentication and L2TP Authentication	342
Authentication Type	342
Local UID	342
Peer UID	342
Password	342
Details	342
Compression	342
Compression/Encryption Stateless Mode	343
L2TP Access Concentrator (for L2TP Authentication only)	343
Add Remote Networks	343
Client Policy	344
Chapter 6	
Servers	345
RADIUS Authentication Servers	345
Enable Access to RADIUS Authentication	346
Remove Suffix from User ID	347
Delimiter Value	347
RADIUS Users Obtain Default Settings from the Group	347
Server Supported Authentication Options	347
Enabled	347

RADIUS Servers	348
Enabled	348
Host Name or IP Address	348
Interface	349
Port	349
Secret	350
Confirm Secret	350
Response Timeout Interval	350
Maximum Transmit Attempts	350
Diagnostics	350
RADIUS Diagnostic Report	350
Internal LDAP Server	351
Server Configuration	351
Internal LDAP Server	351
Switch to External Server	352
General Configuration	352
Remove Suffix from User ID	352
Delimiter Value	352
Internal Server Control	352
Backup/Restore Internal LDAP Database	352
Directory	352
Backup to File	353
Restore from File	353
External LDAP	353
Server Configuration	354
External LDAP Server	354
Switch to Internal Server	355
General Configuration	355
Remove Suffix from User ID	355
Delimiter Value	355
External LDAP Servers	355
Base DN	355
Server	355
Master	356
Slave 1	356

Slave 2	356
Host Name or IP Address	356
Connection	356
Bind DN	357
Bind Password	357
SSL Encryption	357
Certificates	358
RADIUS Accounting Configuration	358
Internal RADIUS Accounting	359
Enable	359
Session Update Interval	359
External RADIUS Accounting Server	359
Interim RADIUS Accounting Record	359
RADIUS Server	360
Test Server	360
Remote User IP Address Pool	361
DHCP	362
Any DHCP Server	363
Specified DHCP Server	363
DHCP Cache Size	363
DHCP Blackout Interval	363
Immediate Address Release	363
Address Pool	364
Pools	364
Start/End	364
Subnet Mask	364
Total	365
In Use	365
Action	365
Address Pool Blackout Interval	365
If Named Pool Unavailable	365
Remote User IP Address Pool Add	366
Starting/Ending	366
Avoid IP Address Pool Conflicts	367
Subnet Mask (optional)	367

Pool	367
Default	367
Existing	367
New	367
Action	368
Server Farm	369
CES Server Farm Mode	370
Enable	370
CES Server Farm Target Server	371
Server IP Address	371
Shasta Sync Port	371
Secret	371
Confirm Secret	371
Keep Alive Parameters	371
Port	371
Interval (sec)	371
Retries	371

Chapter 7

Administration 373

Administrator Settings	374
Primary Administrator	375
User ID	375
Password	376
Settings	376
Idle Timeout	376
Default Language	377
Install Keys	378
Key Installation	378
Feature	378
Key/Status	378
Delete	378
Automatic Backup	378
Restoring Configurations	379
Automatic Backup File Servers	380

Enabled	380
Host	380
Path	380
Specific Time	380
Interval	380
User ID	380
Password	381
Confirm Password	381
Backup	381
Tools	381
Ping	382
Target Address	382
Source Address (Optional)	382
Ping	383
Traceroute	383
Target Address	383
Max Hops (Optional)	383
Wait Timeout (Optional)	383
Traceroute	383
Arp	383
Target Address	383
Arp delete	384
Clear Arp Table	384
Recovery	384
Creating Recovery Diskette	385
Create Diskette	385
Reformat Diskette	386
Using the Recovery Diskette	386
Restore	388
Restore to Device	388
Restore Factory Configuration	388
Restore Backups	388
Reformat Hard Disk	389
Apply New Version	390
Perform File Maintenance	390

View Event Log	390
Set Boot Disk	390
Synchronize Disks	390
Upgrade System Boot Software	390
Restart System	391
Upgrades	391
Current Software	392
Version	392
Build Date	392
Available Updates	392
View	392
FTP New Version From	392
Host	392
Path	392
Version	392
User ID	393
Password	393
Confirm Password	393
Retrieve	393
Apply New Version	393
Version to Apply	393
Apply	394
Current System Configuration	394
Save Current Configuration	395
Name	395
Save	395
Delete Named Configuration	396
Current Named Configurations	396
Restore	396
File System Maintenance	396
Devices	397
Action	398
Display	398
Details	398
Prepare	398

File System Maintenance Details	399
Name	400
Type	400
Size	400
Date	400
Time	400
Action	400
Delete Directory/Delete	400
SNMP	401
SNMP GET HOSTS	403
Enable	403
Host Name or IP Address	403
Community Name	403
Status	403
TRAP HOSTS	403
Enable	403
Host Name or IP Address	404
Community Name	404
Status	404
TRAP CONFIGURATION	404
Enable	404
Description	404
Status	406
Interval	406
Action	406
Click to enable SNMP Authentication traps.	407
Trap Settings	407
SNMP Trap Settings	407
Name	409
Severity	420
Send Once	420
System Shutdown	421
Logins	423
Disable New Logins	423
Disable Logins After Restart	423

System Shutdown	423
After All Users Log Off	423
At	423
In n Minutes	423
Now	424
None	424
After System Shutdown	424
Power Off	424
Restart	424
Boot Mode	424
Boot Configuration	424
Use	424
Reboot From Drive	425
Cancel Pending Shutdown	425
 Chapter 8	
Status	427
Active Sessions	427
Display	428
Summary	429
Current Sessions	429
Peak Sessions for Date	429
Total Sessions Since Boot	429
Current Branch Office Sessions	429
Connection	429
Current End User Sessions	430
User	430
Type	430
User ID	430
IP Address Assigned/Public	430
IPX Address	430
Start	430
Kbytes	430
Packets	431
Links	431

Action	431
Log Off	431
Active Sessions Details	432
Status Reports	434
Graph	435
Reports	436
Type	436
On Screen	437
Comma-Delimited	437
Graphs	437
Graph Type	438
Graph Period	439
Viewing a Single Value	439
Zooming in on a Graph Area	439
Graph	439
Stop	440
Considerations	440
Counters	440
Upgrading and Graphs	440
Bytes In and Bytes Out	440
Historical Graph	440
Reports	440
Tabular Report	441
Comma Delimited Report	443
System Status	443
System Up Time	444
Up Time	444
System Configuration	444
Software Version	444
Software Build Date	445
System Serial Number	445
MAC Address	445
BIOS	445
System Hardware	445
Processors 1 and 2	445

Memory	445
Hard Disk 1 and 2	445
Diskette	446
Health Check	446
Health Check Support	448
Audible Alarm	448
Enable	448
Disable	448
Component Name	448
Status	448
Description	449
More Information	449
Additional Information for Health Check screen	449
Health Check Components	449
Alert and Warning Descriptions for Selected Servers	451
Statistics	453
Buttons	454
Version	454
Tasks	454
Interfaces	454
Stack	455
Memory	455
ARP Table	455
Route Table	455
Sockets	455
TCP Stats	455
UDP Stats	455
ICMP Stats	455
IP Stats	456
Mbuf Stats	456
File System	456
Devices	456
LAN Counters	456
WAN Status	457
Security Stats	457

Slapd	457
Flash Contents	457
Object List	457
Config File	458
IP Addr Pool	458
PACE Statistics	458
Event Objects	458
IPX Route Table	458
IPX Server Table	458
IPX Stats	458
FIPS	458
Load Balancing	458
Check Point FW-1 Stats	459
Check Point FW-1 Version	459
Check Point FW-1 Info	459
Firewall	459
Host	460
Interface	460
Policy	460
Date	461
Statistics	461
Accounting	461
Accounting Records	462
Display	462
Search	463
Session Fields	464
Name	464
Subnet	464
Time	464
Date	464
Packets	465
Kbytes	465
Session ID	465
User ID	465
IP Address	465

IPX Address	465
Links	465
Historical Event Logging	466
Common Logging Fields	467
Date	467
Display Level	468
Normal	468
Urgent	468
Detailed	468
All	468
Display	469
Entries	469
Event Log	470
IP/IPX Packet Drops	471
All Packets	471
Filtered Packets	471
Clear	471
Refresh	471
System Log	471
System Log Contents for Date	472
Capture Level	473
Normal	473
Urgent	473
All	473
Security Log	473
Configuration Log	475
Index	477

Figures

Figure 1	System menu	55
Figure 2	System Identity	56
Figure 3	LAN Interfaces	59
Figure 4	Edit LAN Interface	63
Figure 5	Edit LAN Interface – Slot n Interface n	64
Figure 6	Edit IP Address – LAN Interface	66
Figure 7	Edit IP Address – Slot n Interface n	67
Figure 8	Sample LAN Interface Statistics screen	72
Figure 9	WAN Interfaces screen	75
Figure 10	WAN Statistics screen	78
Figure 11	Configure WAN Interface Settings screen	81
Figure 12	CSU/DSU	85
Figure 13	Local Authentication	88
Figure 14	WAN Interface Advanced Settings	90
Figure 15	SystemÆIPX Configuration	93
Figure 16	Hardware Accelerator	96
Figure 17	Hardware Accelerator Configuration	98
Figure 18	Date and Time	102
Figure 19	Network Time Protocol	103
Figure 20	Add/Edit NTP server screen	105
Figure 21	Installed Certificates	107
Figure 22	Create New Key and Certificate Request	110
Figure 23	Generated PKCS#10-encoded Certificate Request	112
Figure 24	Paste PKCS #7 Base-64 Certificate	113
Figure 25	Certificate Details	115
Figure 26	SystemÆSwitch Settings	118
Figure 27	System Forwarding	122
Figure 28	Services menu	125
Figure 29	Available Services	126

Figure 30	IPSec Server	130
Figure 31	PPTP Server	137
Figure 32	L2TP Server	139
Figure 33	L2TP Add or Edit	141
Figure 34	L2F Settings	143
Figure 35	L2F Add Network Access Server	145
Figure 36	RADIUS Service	147
Figure 37	Add RADIUS Service Client Screen	150
Figure 38	ServicesÆFirewall/NAT screen	152
Figure 39	Check Point FireWall-1 Service screen	159
Figure 40	SYSLOG Forwarding	164
Figure 41	Routing Menu	167
Figure 42	Static Routes Configuration	168
Figure 43	Static RoutesÆEdit	170
Figure 44	Static RouteÆAdd Public Default Route screen	171
Figure 45	Static RoutesÆAdd Private Default Route	172
Figure 46	Static RoutesÆEdit Static Route	174
Figure 47	Static RoutesÆAdd Static Route screen	175
Figure 48	Static RoutesÆBranch Office	176
Figure 49	RoutingÆOSPF	179
Figure 50	RoutingÆOSPFÆEdit Area	181
Figure 51	RoutingÆOSPFÆLSDB	183
Figure 52	RoutingÆOSPFÆNeighbor	184
Figure 53	OSPFÆInterfaces screen	185
Figure 54	OSPFÆSummary	186
Figure 55	OSPFÆStatistics	187
Figure 56	RIP	189
Figure 57	RIPÆStatistics	190
Figure 58	RIP database	191
Figure 59	RIPÆInterfaces	192
Figure 60	Routing Interfaces	194
Figure 61	Routing InterfacesÆConfigure OSPF	195
Figure 62	Routing InterfacesÆConfigure RIP	198
Figure 63	Routing InterfacesÆConfigure VRRP	201
Figure 64	VRRP screen	205

Figure 65	VRRPÆCreate/Edit VRRP IP Address	207
Figure 66	VRRPÆConfiguration	210
Figure 67	VRRPÆStatistics	212
Figure 68	VRRPÆErrors	213
Figure 69	Route table filter criteria screen	215
Figure 70	Route TableÆIP Forward Table Screen	217
Figure 71	Route TableÆRoute Table	218
Figure 72	Access List	220
Figure 73	Access ListÆCreate	221
Figure 74	Access ListÆEdit	222
Figure 75	Routing Policy Service	224
Figure 76	PolicyÆAdd	226
Figure 77	Client Address Redistribution	228
Figure 78	Client Addr RedistÆUser Tunnel Routes	230
Figure 79	Routing Status	232
Figure 80	QOSÆCurrent Multi-Field (MF) Classifiers	236
Figure 81	QOSÆRules	238
Figure 82	ClassifiersÆRulesÆEdit/Create Rules	239
Figure 83	QoS Interfaces	242
Figure 84	QoS InterfacesÆBandwidth ManagementÆConfigure	243
Figure 85	QoS InterfacesÆDiffServÆConfigure	245
Figure 86	QoS InterfacesÆEgress Queueing Mode	247
Figure 87	QoS Bandwidth Management	248
Figure 88	Bandwidth Rates	249
Figure 89	Profiles Menu	251
Figure 90	Groups	253
Figure 91	GroupsÆAdd	255
Figure 92	Group Configuration Edit screen (Default Attributes)	257
Figure 93	Groups Edit Connectivity	258
Figure 94	Partial IPSec Edit	265
Figure 95	PPTP Edit	276
Figure 96	L2TP Edit	278
Figure 97	L2F Edit	279
Figure 98	User Management Group Profile	284
Figure 99	Partial User Add or Edit	287

Figure 100	IPSec Subnet Mask Assignment	290
Figure 101	Filters	295
Figure 102	Copy Filters	297
Figure 103	Manage Rules	302
Figure 104	Create Filters Rule Definition	304
Figure 105	Edit Filter Rule Definition	305
Figure 106	Current Addresses	310
Figure 107	Create or Edit Addresses	311
Figure 108	Current Protocols	313
Figure 109	Create or Edit Protocols	314
Figure 110	Current Ports	315
Figure 111	Create or Edit Port	316
Figure 112	Hours of Access	317
Figure 113	Edit Hours of Access	319
Figure 114	Networks	320
Figure 115	Networks Edit	322
Figure 116	Domain	323
Figure 117	Edit Domains	325
Figure 118	Branch Office	328
Figure 119	Branch OfficeÆEditÆIP	332
Figure 120	Define Connection	335
Figure 121	Add Remote Networks	344
Figure 122	Servers Menu	345
Figure 123	RADIUS Authentication Servers	346
Figure 124	Internal LDAP Server	351
Figure 125	External LDAP Server	354
Figure 126	RADIUS Accounting Configuration	358
Figure 127	Remote User IP Address Pool	362
Figure 128	Internal Address Pool Add	366
Figure 129	Shasta Server Farm	370
Figure 130	Administration Menu	373
Figure 131	Administrator Settings	375
Figure 132	Automatic Backup	379
Figure 133	AdminÆTools	382
Figure 134	Create Recovery Diskette Display	385

Figure 135 Recovery Diskette	387
Figure 136 Upgrades	391
Figure 137 Current System Configuration	395
Figure 138 File System Maintenance	397
Figure 139 File System Maintenance Details	399
Figure 140 SNMP	402
Figure 141 SNMP Trap Settings	408
Figure 142 System Shutdown	422
Figure 143 Status Menu	427
Figure 144 Active Sessions	428
Figure 145 Partial Active Sessions Details	432
Figure 146 Status Reports	435
Figure 147 System Resources Graph	438
Figure 148 Users Report	442
Figure 149 Comma Delimited Report	443
Figure 150 System Status	444
Figure 151 Health Check	447
Figure 152 Statistics	454
Figure 153 Check Point FireWall-1 Status	460
Figure 154 Partial Accounting	462
Figure 155 Nortel Networks Logging Scheme	467
Figure 156 Event Log	470
Figure 157 System Log	472
Figure 158 Security Log	474
Figure 159 Configuration Log	475

Tables

Table 1	Description of Fields	73
Table 2	Software-level packet data	74
Table 3	WAN Statistics	79
Table 4	Packet Data Statistics	80
Table 5	Management Protocols	128
Table 6	Comparing Encryption and Authentication Methods	132
Table 7	Check Point FireWall-1 states	161
Table 8	OSPF LSDB	183
Table 9	OSPF Dynamic Neighbors	184
Table 10	OSPF interfaces	185
Table 11	OSPF Summary	186
Table 12	OSPF Statistics	188
Table 13	RIP statistics	190
Table 14	RIP database	191
Table 15	RIP Interfaces	193
Table 16	VRRP configuration information	211
Table 17	VRRP Statistics	212
Table 18	VRRP Errors	213
Table 19	IP Forward Table Screen	217
Table 20	IP Routing Table	219
Table 21	Client address redistribution statistics	231
Table 22	Wildcard examples	312
Table 23	Load balancing service trap messages	410
Table 24	Internal LDAP server trap messages	410
Table 25	RADIUS accounting server trap messages	411
Table 26	RADIUS authentication server trap messages	411
Table 27	External LDAP servers trap messages	412
Table 28	Dual power supply trap message	413
Table 29	Intrusion trap message	413

Table 30	Critical temperature trap message	414
Table 31	Normal temperature trap message	414
Table 32	Voltage trap messages	415
Table 33	Chassis Fan 2 trap message	416
Table 34	Chassis fan trap message	417
Table 35	CPU two fan trap messages	417
Table 36	CPU one fan trap messages	418
Table 37	CPU 2 trap message	418
Table 38	FIPS trap messages	419
Table 39	DNS servers trap messages	420
Table 40	Severity Level Meanings	420
Table 41	Descriptions of Active Session Details	433
Table 42	Health Check Components	449
Table 43	Health Check Messages from SNMP Traps	451
Table 44	WAN Status Values	457

Preface

This book is intended for Nortel Networks™ Contivity® VPN Switch managers. It provides reference information for each of the Web browser configuration screens.

Before you begin

This guide is for network managers who are responsible for setting up and managing the Contivity VPN Switch. This guide assumes that you have the following background:

- Experience with windowing systems or graphical user interfaces (GUIs)
- Familiarity with network management

This guide refers to the Contivity VPN Switch as the switch.

Text conventions

This guide uses the following text conventions:

angle brackets (< >) Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command.

Example: If the command syntax is
`ping <ip_address>`, you enter
`ping 192.32.10.12`

bold Courier text Indicates command names and options and text that you need to enter.

Example: Use the **ping** command.

braces ({})	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is <code>show ip {alerts routes}</code>, enter either <code>show ip alerts</code> or <code>show ip routes</code>, but not both.
brackets ([])	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is <code>show ip interfaces [-alerts]</code>, you can enter either <code>show ip interfaces</code> or <code>show ip interfaces -alerts</code>.
ellipsis points (. . .)	Indicate that you repeat the last element of the command as needed. Example: If the command syntax is <code>ethernet/2/1 [<parameter> <value>] . . .</code>, you enter <code>ethernet/2/1</code> and as many parameter-value pairs as needed.
<i>italic text</i>	Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is <code>show at <valid_route></code>, <i>valid_route</i> is one variable and you substitute one value for it.
plain Courier text	Indicates command syntax and system output, for example, prompts and system messages. Example: Set Trap Monitor Filters

arrow (→)	Shows menu paths. Example: Protocols→IP identifies the IP option on the Protocols menu.
vertical line ()	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is <code>show ip {alerts routes}</code> , you enter either <code>show ip alerts</code> or <code>show ip routes</code> , but not both.

Related publications

For more information about using the Contivity VPN Switch, refer to the following publications:

- Release notes for the switch (part number 301459-T) and the client (part number 301459-V) provide the latest information, including brief descriptions of the new features, problems fixed in the this release, and known problems and workarounds.
- *Configuring the Contivity VPN Switch* (part number 3116423-C) provides information for configuring, maintaining and troubleshooting the switch.
- *Reference for the Contivity VPN Switch Command Line Interface* (part number 311645-B) describes the commands that you can use from the command line interface.
- *Managing the Contivity Stateful Firewall* (part number 312538-A) describes firewall concepts, how to configure and monitor the firewall, and the firewall commands that you can use from the command line interface.
- *Installing the Extranet Access Client* (part number 311644-A) provides procedural information to help you configure, monitor, and troubleshoot your switch.

You can print selected technical manuals and release notes free, directly from the Internet. Go to the www.nortelnetworks.com/documentation URL. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe Acrobat Reader to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe* at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader*.

You can purchase selected documentation sets, CDs, and technical publications through the Internet at the www1.fatbrain.com/documentation/nortel/ URL.

Hard-copy technical manuals

You can print selected technical manuals and release notes free, directly from the Internet. Go to the support.baynetworks.com/library/tpubs/ URL. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe Acrobat Reader to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems at www.adobe.com to download a free copy of Acrobat Reader.

You can purchase selected documentation sets, CDs, and technical publications though the Internet at www1.fatbrain.com/documentation/nortel/ URL.

How to get help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	Telephone
EMEA	(33) (4) 92-966-968
North America	(800) 2LANWAN or (800) 252-6926

Technical Solutions Center	Telephone
Asia Pacific	(61) (2) 9927-8800
China	(800) 810-5000

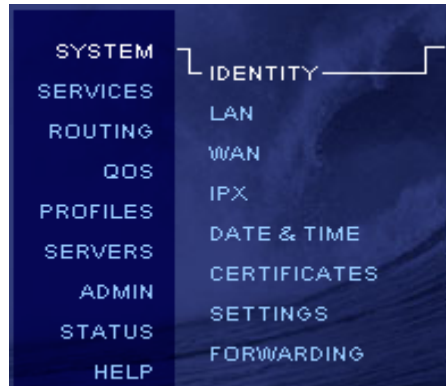
An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the www12.nortelnetworks.com/ URL and click ERC at the bottom of the page.

Chapter 1

System

The System menu provides access to screens for configuring various system level settings.

Figure 1 System menu



System Identity

Each Contivity VPN switch is uniquely identified by the system's address and domain name system (DNS) name. The DNS name can be used instead of the IP address to identify the switch and launch its management interface through a Web browser.

The System Identity screen allows you to optionally change your switch Management IP address, and provide the DNS Host Name and Domain Name. Additionally, you can assign up to three DNS addresses to resolve IP address name resolution requests.

You can also reset the switch Management IP address values using the serial interface.

Figure 2 System Identity

The screenshot shows a web browser window titled "Corinity Ethernet Switch - Microsoft Internet Explorer". The address bar shows "http://10.0.16.143/manage/manager.htm". The page has a dark blue sidebar with a menu: SYSTEM, SERVICES, PROFILES, SERVERS, ADMIN, ROUTING, STATUS, HELP, and CERTIFICATES. The "IDENTITY" section is selected. The main content area is titled "System Identity" and contains the following fields:

- Management IP Address:** 10.0.16.143 (Web Management, FTP, etc. Subnet 255.255.0.0)
- Domain Identity:**
 - DNS Host Name:** PDTarget
 - DNS Domain Name:** (empty)
- DNS Server Address:**

	Primary	Secondary	Tertiary	
	0.0.0.0	0.0.0.0	0.0.0.0	Server not configured
		*Optional	*Optional	Server not configured
				Server not configured

At the bottom are buttons for OK, Cancel, and Refresh. The Nortel Networks logo is in the bottom left corner.

System Identity

Management IP Address

Enter a Management IP Address for the system. You need this address to contact all system services, such as HTTP, FTP, and SNMP. To be accessible, the Management IP Address must map to the same network as one of the private interfaces.

For example, if you are planning on assigning IP address 10.2.3.3 with the subnet mask 255.255.0.0 to the private physical interface, the Management IP Address must reside in the 10.2.x.x network.

Changing IP Addresses

If you configure the switch on one network and plan to move it to another network, change the Management IP address and private LAN interface addresses before moving the switch. Then, communicate with the switch using the new Management IP address from your browser's URL address field.

Domain Identity

DNS Host Name

Enter a Name to identify the system. This should be the same name that is used by the DNS server to identify the management address of the switch that is located on your private network. You can enter up to 64 characters maximum.

DNS Domain Name

Enter the Name of the Internet Domain into which this system is being placed. This must be the same Internet Domain as the System Name in the Domain Name System (DNS) server.

A domain is a part of the Internet naming hierarchy that refers to general groupings of networks that are based on organization-type or geography. For example, mycompany.com is the domain name for a commercial (.com) enterprise.

DNS Server Address

Primary

Enter the address of the DNS server that is located on your private network. The DNS server translates textual host names into IP addresses. For example, DNS can translate the fully qualified host name *www.mycompany.com* to its IP address 192.19.2.33.

The Primary DNS server is the first one addressed for servicing name resolution requests that are needed by the system; if the Primary DNS server is unavailable, service is requested of the Secondary DNS server.

This is the DNS entry that management tools use to resolve names in configurations. Always use the IP address for setting a DNS server host instead of a domain name.



Note: If no DNS servers are specified, management requests that are using names rather than network addresses fails.

Secondary

Enter an address for the Secondary Domain Name System (DNS) server. If the Primary DNS server is unavailable, service is requested of the Secondary DNS server (if present).

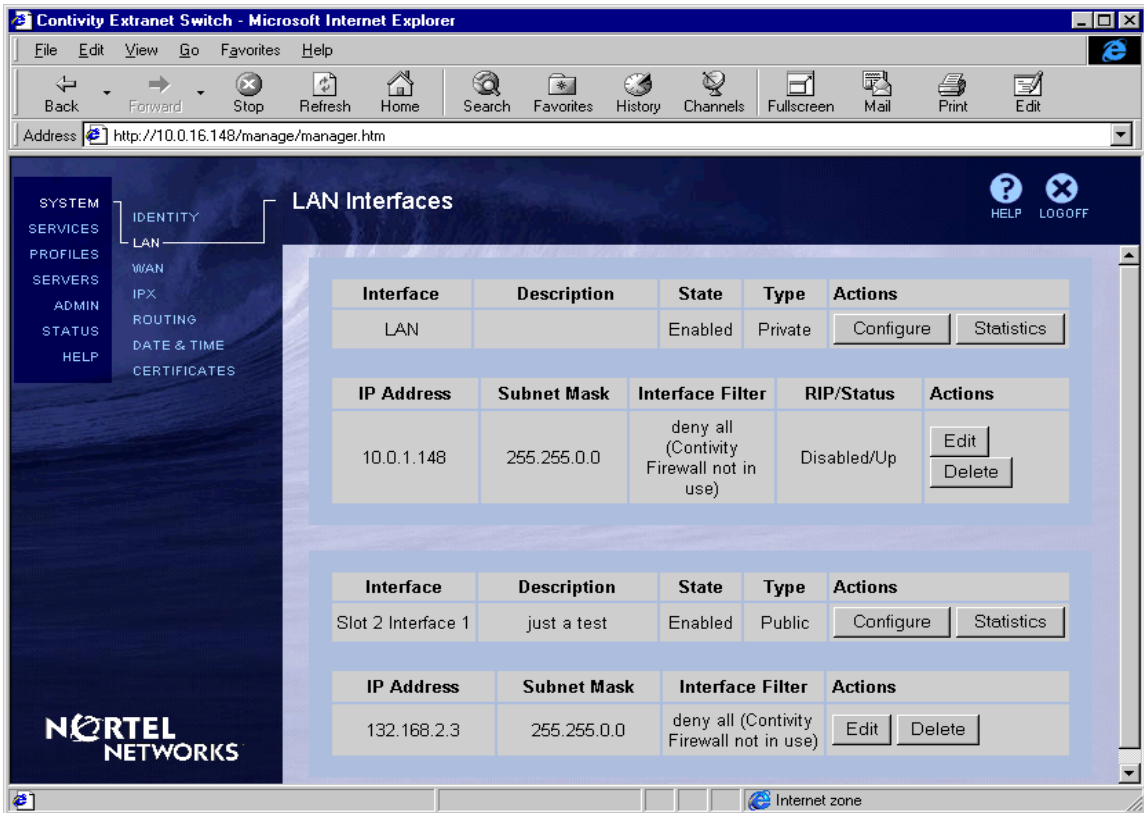
Tertiary

Enter an address for the Tertiary Domain Name System (DNS) server. If the Primary and Secondary DNS servers are unavailable, service is requested of the Tertiary DNS server (if present).

LAN Interfaces

The LAN Interfaces screen shows the interfaces that have been detected in the switch. The screen provides information about the interfaces, including the current state and Type (Private or Public). In addition, it shows the IP address, the status of the Contivity Firewall, the interface filters that are being used, and the status of RIP on the interface. You can also configure the interface or view statistics on it from this screen.

Figure 3 LAN Interfaces



LAN/WAN IP Addressing

The private LAN interface and the Management IP Address must be on the same network, and the public LAN interface should be on a different network, both physically and logically.

If your switch has a single network interface and you want to position the switch behind the firewall and router, then you should set the switch's interface type to Private.

Interface

LAN represents the Ethernet interface on the system board, which is installed on every switch.

Slot *n* Interface *n* represents an optional local area network card in expansion Slot *n* using Interface *n*.

Description

Shows the interface description (for example, the Private Interface), if one has been provided on the Interface Configuration screen (for example, a site, location, address, user name, or configuration tag). This can be helpful for network administrators working with the switch after it has been configured.

State

Enabled

This LAN interface is currently available.

Disabled

This LAN interface is currently unavailable.

Type

Public

Indicates that this interface is attached to a public data network like the Internet. The switch rejects nontunneled protocols and only accepts tunneled protocols like IPSec, PPTP, L2TP, L2F, and the diagnostic protocol PING on a Public interface.

A host can send only enough packets to a Public interface to establish a tunnel connection. If the tunnel is not established before a preset maximum number-of-packets-allowed counter is reached, then the packets from that host are discarded.

Private

Indicates that this interface is attached to the Private network and it can accept nontunneled networking protocols such as TCP/IP, FTP, and HTTP. The Private interface also accepts tunneled protocols (for example, IPSec, PPTP, L2TP, L2F) that can be used for secure management access to the switch.



Note: The private LAN interface and the Management IP address should be on the same network, and the public LAN interface should be on a different network, both physically and logically.

If you have one network only and want to position the switch behind the firewall and router, then you should use a private LAN interface only (do not use a public LAN interface).

Actions

Configure

Click to modify the interface characteristics.

Statistics

Click to view the Link Statistics.

Edit

Click to change any of the LAN Interface attributes for the associated device.

Delete

Click to remove the listed IP address and associated information attached to the interface. You cannot delete the Management IP address from the switch.

IP Address

Shows the current IP Address that is assigned to the interface.

Subnet Mask

The Subnet Mask defines which bits of the IP address represent the network the device is on and which bits represent the host's ID on the network.

The device uses the Subnet Mask to determine which IP addresses are directly reachable on the network and which must be routed through a gateway. A sample IP address is 10.2.3.3 with a Subnet Mask of 255.255.0.0. This indicates that all hosts with addresses 10.2.*n.n* are directly reachable.

Interface Filter

Shows whether the Contivity Firewall is in use on this LAN interface (this reflects the selection on the Services→Firewall screen).

This entry also shows the interface filter that is currently being used by the Contivity Firewall. This is the interface filter that is selected on the System→LAN Interfaces→Edit IP Address screen. If no interface filter has been selected, the default of Deny All is used.

Edit LAN Interface

The Configure button on the LAN Interfaces screen (System→LAN Configure) allows you to provide optional information for the LAN Interfaces, such as a description. This information then appears on the System→LAN screen. Additional fields appear on the Edit LAN Interface screen for optional network cards.

Figure 4 Edit LAN Interface

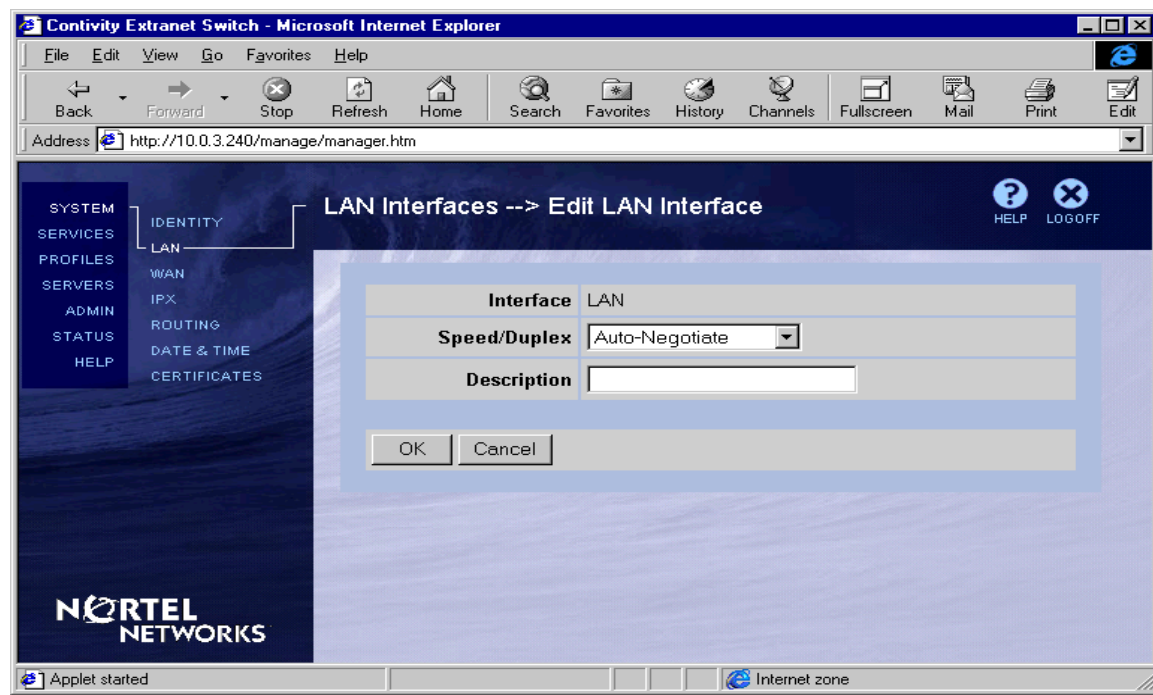
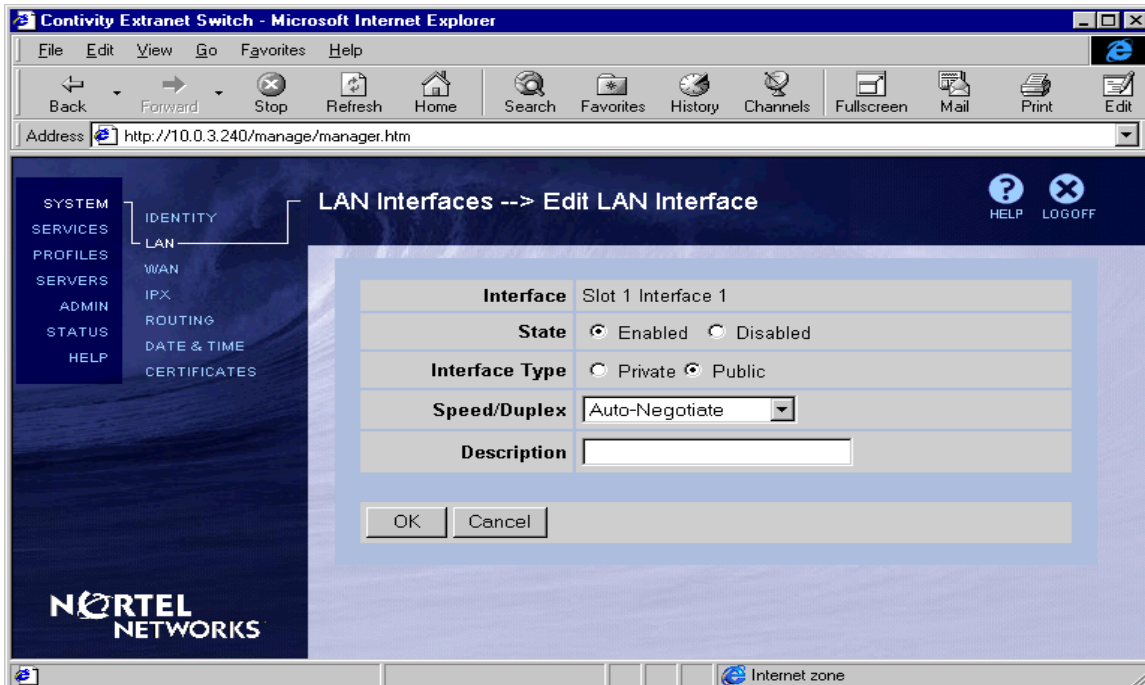


Figure 5 Edit LAN Interface – Slot *n* Interface *n*

Interface

LAN represents the physical port interface to which you assign an IP address.

Slot *n* Interface *n* represents an optional LAN card in expansion Slot *n* using Interface *n*.

Speed/Duplex

Use the Speed/Duplex field to automatically or manually configure the LAN interface's port speed and mode.



Note: You can also use the Interface selection on the switch's Serial Port menu to set autonegotiation.

Select Auto-Negotiate to specify that the switch automatically set the port speed and mode to match the best service provided by the connected station, up to 100 Mbps in full-duplex mode. Auto-Negotiate is the default selection, and complies with the IEEE 802.3u autonegotiating standard.

Select one of the following selections to manually set the LAN interface's port speed and mode to match the speed and mode used by the connected station.

- 100Mbps/Full duplex
- 100Mbps/Half duplex
- 10Mbps/Full duplex
- 10Mbps/Half duplex



Note: You might not be able to connect to the remote system if the system is not using autonegotiation or if it uses an incompatible form of autonegotiation. If this occurs, manually set your switch's speed and mode settings to match those used by the remote system.

Description

An optional description that you can provide for the LAN Interface. The description appears on the LAN Interfaces screen.

State

The State field appears on the screen for an optional LAN card in expansion Slot *n* using Interface *n*. Click to enable or disable the card.

Interface Type

The Interface Type field appears on the screen for an optional LAN card in expansion Slot *n* using Interface *n*. Click to specify whether the interface is public or private.

Add IP Address and Edit IP Address

The Add IP address screen (System→LAN Add) allows to you assign an IP Address and Subnet Mask to the interface. Use the Edit IP Address screen (System→LAN Edit) to modify the information. The Add and Edit screens are also used to specify routing-related settings and to specify the interface filter used for the Contivity Firewall.

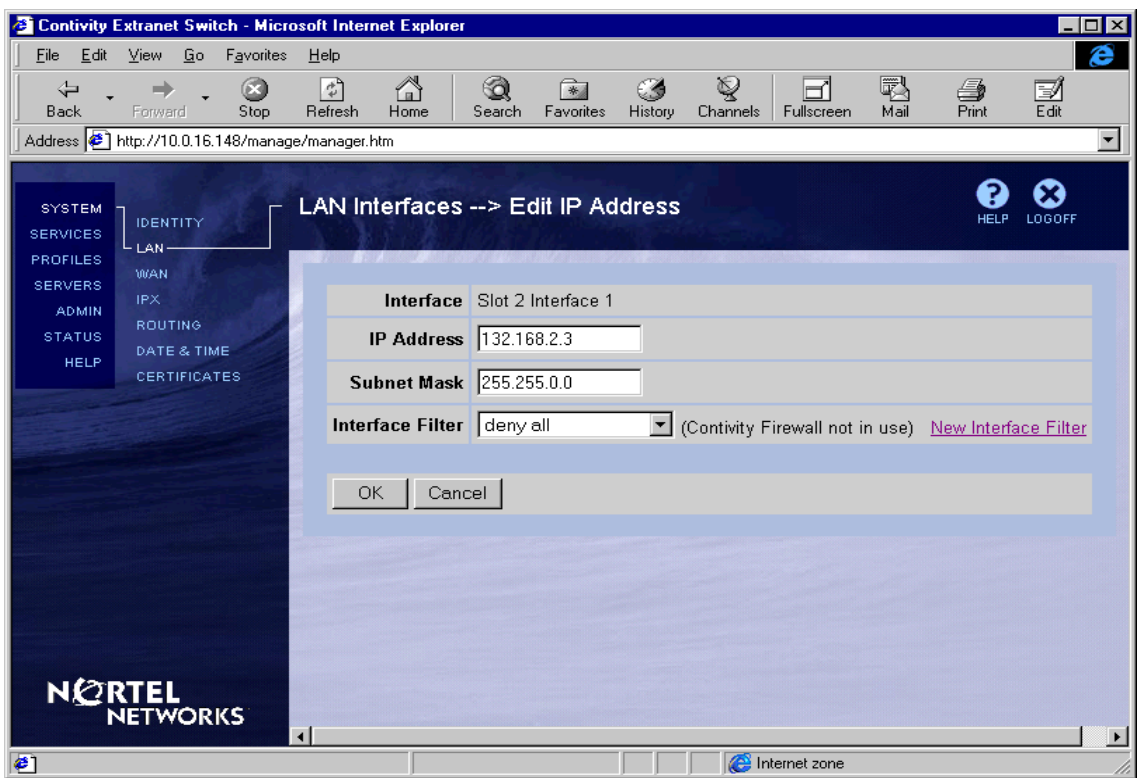
Figure 6 Edit IP Address – LAN Interface

The screenshot displays the 'Edit IP Address' configuration page for a LAN interface. The browser window is titled 'Contivity External Switch - Microsoft Internet Explorer'. The address bar shows 'http://10.0.15.140/manage/manage.htm'. The left sidebar contains a navigation menu with options: SYSTEM, SERVICES, PROFILE, SERVERS, ADMIN, STATUS, and LOG. The main content area is titled 'LAN Interfaces --> Edit IP Address'. It features a form with the following fields and options:

- Interface:** LAN
- IP Address:** 10.0.1.140
- Subnet Mask:** 255.255.0.0
- Interface Filter:** deny all (Contivity Firewall not in use) [New Interface Filter](#)
- Routing Information Protocol (RIP):**
 - Enabled:** ☐
 - Transmit Mode:** V2
 - Receive Mode:** V2
 - Simple:** ☐
 - Authentication:** Password: Confirm Password:
 - Import Default Route:** ☐
 - Poison Reverse:** ☒
 - Export Default Routes Metric:** Disabled
 - Export Static Routes Metric:** Disabled
 - Export Branch Office Static Routes Metric:** 1

At the bottom of the form are 'OK' and 'Cancel' buttons. The Nortel Networks logo is visible in the bottom left corner of the interface.

Figure 7 Edit IP Address – Slot *n* Interface *n*



Interface

LAN - Represents the physical port interface to which you assign an IP address.

Slot *n* Interface *n* - Represents an optional LAN card in expansion Slot *n* using Interface *n*.

IP Address

The IP Address for the interface. The IP Address consists of 32 bits, which are written as four octets (8-bit bytes) in dotted-decimal format. For example:

192.168.34.21

Subnet Mask

The Subnet Mask defines how many bits of the IP Address represent the network the device is on and how many bits represent the host's ID on the network.

The device uses the Subnet Mask to determine which IP Addresses are directly reachable on the network and which must be routed through a gateway. A sample IP Address is 10.2.3.3 with a Subnet Mask of 255.255.0.0. This indicates that all hosts with addresses 10.2.*n.n* are directly reachable.

Interface Filter

Shows whether or not the Contivity Firewall is in use (this reflects the selection on the Services→Firewall screen).

This entry also shows the interface filter that is currently being used by the Contivity Firewall. Use the dropdown menu to show a list of all interface filters that have been set up on the switch (on the Profiles→Filters screen), and to select a different filter for the Contivity Firewall.



Note: If you change the interface filter setting, a message informs you that you must restart your switch before the new interface filter is used. If the Contivity Firewall is not enabled, the new selection has no effect.

Use the New Interface Filter link to go to the Profiles→Filters screen and create a new filter.

The default Interface Filter setting is Deny All.

Routing Information Protocol (RIP)

In addition to the previously-described fields, the Add IP Address and Edit IP Address screens for the switch's LAN interface are also used to specify routing-related information for the private network.

The private LAN uses Routing Information Protocol (RIP) for routing traffic within the private network. RIP is a distance-vector protocol that enables routers to exchange routing information by means of periodic RIP updates. Routers transmit their own RIP updates to neighboring subnets and listen for RIP updates from the routers on those neighboring subnets. Routers use the information in the RIP updates to keep their internal routes current.

For RIP, the “best” path to a destination is the path with the fewest hops. RIP computes distance as a metric, usually the number of hops (or routers) from the origin subnet to the target subnet. RIP can handle a maximum of 15 hops.

Enabled

Indicates that the RIP specifications on this screen have been enabled. You must also have the global Enabled specification selected on the System→Routing screen. The default on this screen is Disabled.

Transmit

The Transmit Mode enables you to specify which version of the RIP protocol is used when routing traffic from this switch. The default of V2 indicates RIP-2. You can select V1 to specify that RIP-1 traffic is sent.

A selection of **OFF** specifies that RIP is not used. In this case the static routes that are set on the System→Routing screen are used.

Receive

The Receive Mode enables you to specify which version of the RIP protocol the switch accepts for incoming traffic. The default of V2 indicates that only RIP-2 traffic is accepted. You can select V1 to specify that RIP-1 is accepted.

A selection of **OFF** specifies that RIP traffic is not accepted. The static routes set on the System→Routing screen are used. A selection of **BOTH** specifies that incoming transmissions using either version of RIP are accepted.

Authentication

Indicates the type of authentication that is used as part of the RIP transmission. This authentication is specific to the RIP routing protocol and has no bearing on the authentication done as part of the connection to the switch. The default is None, which specifies that no authentication is required.

SIMPLE indicates that authentication is accomplished through the use of a simple password. MD5 specifies that authentication is accomplished by using a MD5 secret.

If you select either Simple or MD5, password and confirmation fields display below the selection.

Import Default Route

Typically, you specify a default route in the switch's Routing Table (System→Routing). The switch then uses that default route when sending traffic to the public network. However, if no default route has been set, you can check the Import Default Route box and the switch uses the default route that it learned during RIP updates.

Poison Reverse

Click to enable or disable poison reverse. (Poison reverse updates remove routing loops in large networks.)

Export Default Routes Metric

Use this field to specify that the switch's default route is exported during RIP updates. You can also assign a metric value to the default route.

Export Static Routes Metric

Use this field to specify that the switch's static routes are exported during RIP updates. You can also assign a metric value to the routes.

Export Branch Office Static Routes Metric

If you have a branch office connection, use this field to export the static routes metric. This informs the remote branch office connection of the routes that are used for the connection and provides the metric value you assign to the routes.

LAN Interface Statistics screen

This screen (System→LAN Statistics) provides key counters and can help you diagnose and troubleshoot problems with your LAN interfaces.

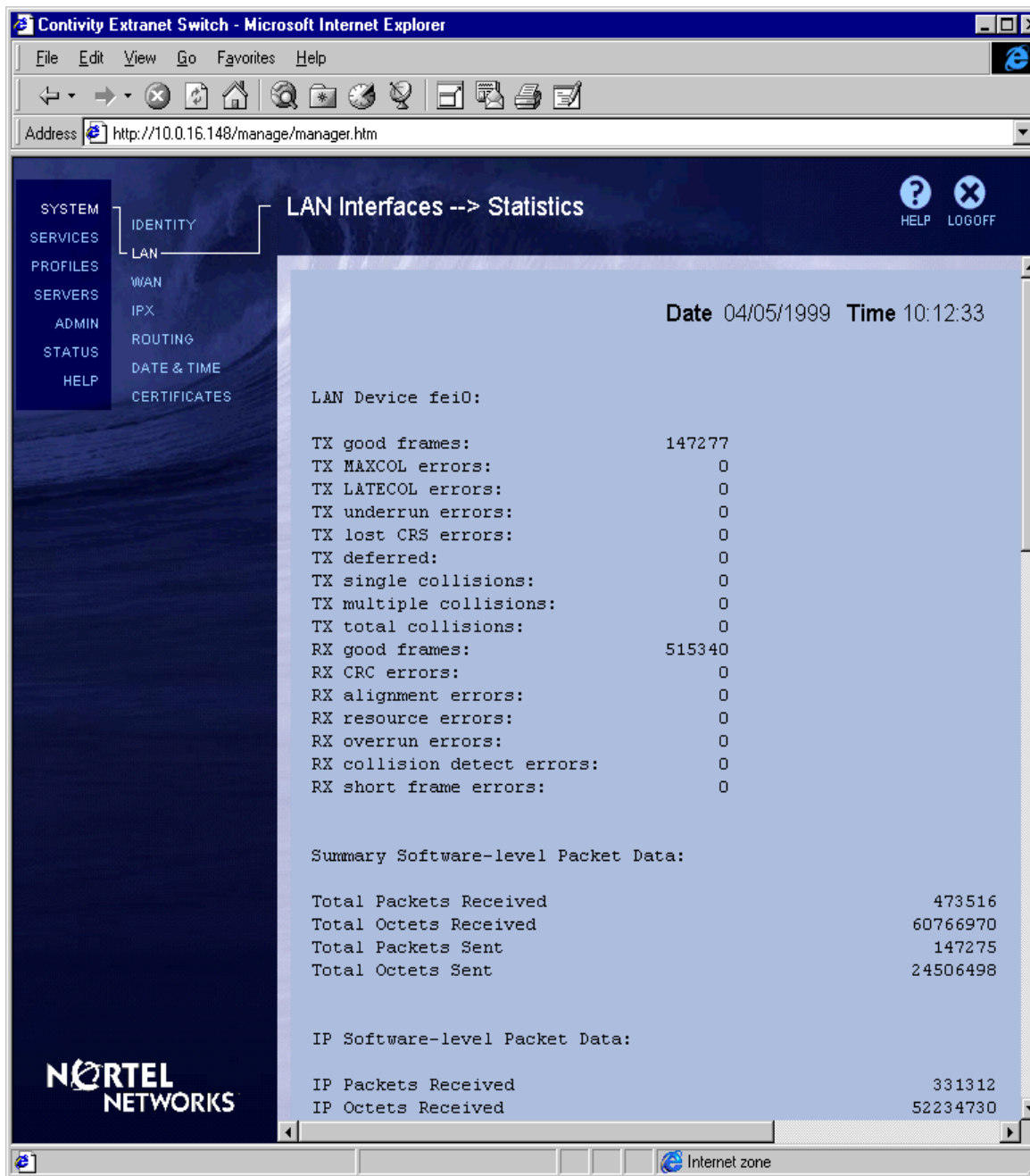
Figure 8 Sample LAN Interface Statistics screen

Table 1 Description of Fields

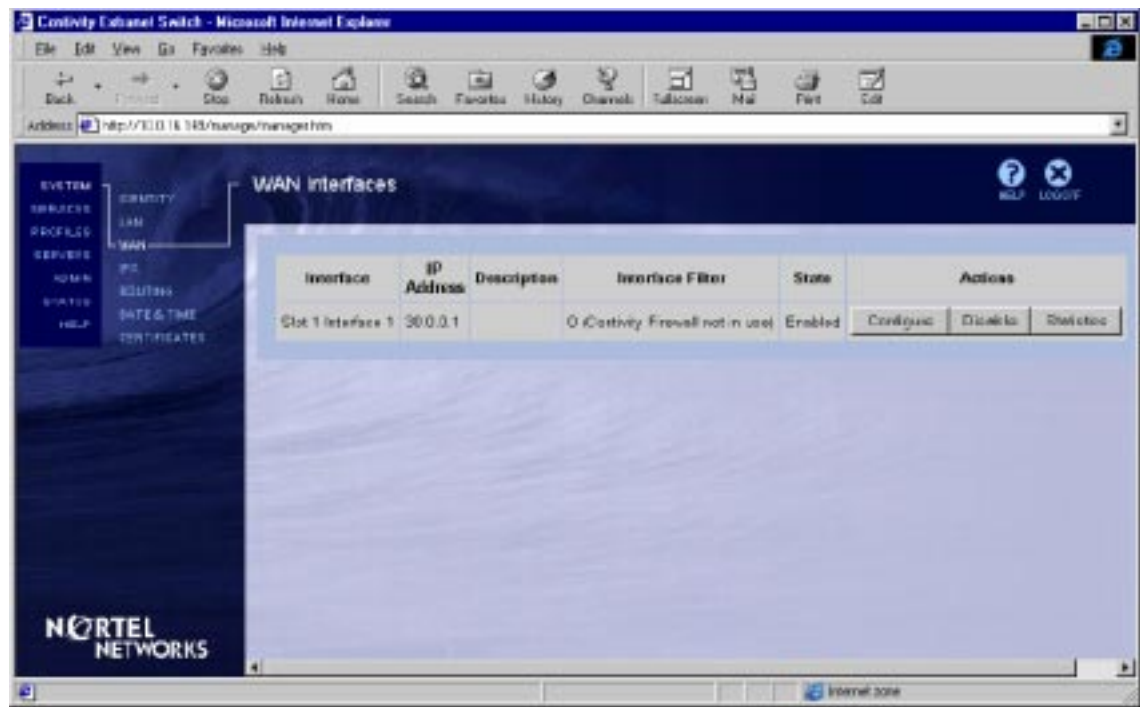
LAN Device	Description
Tx good frames	Good frames transmitted.
Tx MAXCOL errors	The number of frames not transmitted because the frame reached the maximum allowable collision threshold.
Tx LATECOL errors	The number of frames not transmitted because they experienced a late collision during transmission.
Tx underrun errors	The number of frames not transmitted because the hardware transmitter experienced a buffer underrun during transmission.
Tx lost CRS errors	The number of frames not transmitted because carrier sense was lost during transmission.
Tx deferred	The number of times a frame was deferred due to a collision during transmission.
Tx single collisions	The number of times a single collision occurred during a frame transmission.
Tx multiple collisions	The number of times multiple collisions occurred during frame transmissions.
Tx total collisions	Total collisions that occurred during frame transmission.
Rx good frames	Good frames received.
Rx CRC errors	The number of received frames discarded due to an invalid cyclic redundancy check error.
Rx alignment errors	The number of received frames discarded due to invalid frame alignment.
Rx resource errors	The number of frames discarded because a buffer was not available to receive the frame.
Rx overrun errors	The number of received frames discarded because the hardware receiver experienced an overrun error during reception.
Rx collision detect errors	The number of received frames discarded due to a collision error during reception.
Rx short frame errors	The number of received frames discarded because they didn't meet the minimum frame length.

Table 2 Software-level packet data

Software-level packet data	Description
IP Fragments Received	IP fragments received.
IP Routing Filter Drops	Routing filter drops occur when packets are filtered because no access rights are permitted to the resources specified by the designated filters.
IP Local System Filter Drops	Local system filter drops occur when packets are destined to the management interface but are dropped due to lack of authorization access.
IP Local Interface Filter Drops	Local interface filter drops occur when packets are destined to a physical interface but are dropped due to lack of authorization access.
IP PAT Drops	Public Address Table (PAT) drops represent the number of packets dropped prior to being authenticated and having a tunnel established on a public interface.
IP Header Error Drops	IP header error drops occur whenever there is an error in the IP header.

The WAN interfaces screen (System→WAN) shows the WAN interfaces currently installed in the switch, the slot in which the cards reside, an interface description (if one has been provided), and the current state. It also indicates whether the Contivity Firewall is active and the interface filter that is in use. From this screen, you can move to another screen to configure or disable a WAN card, or view statistics.

Figure 9 WAN Interfaces screen



Interface

Slot *n* Interface *n* represents an optional wide area network (WAN) card in expansion Slot *n* using Interface *n*.

IP Address

The IP Address for the interface.

 **Note:** To change the IP address of a WAN link, you must disable the interface, change the address and re-enable the interface. This automatically disables static routes for the interface. If you change the IP address back to the original address, you must manually re-enable static routes.

Description (Optional)

A description that you can optionally provide. For example, a site, location, address, user name, or configuration tag. This can be helpful for network administrators working with the switch after it has been configured.

Interface Filter

Shows whether the Contivity Firewall is in use on this WAN interface (this reflects the selection on the Services→Firewall screen).

This entry also shows the interface filter that is currently being used by the Contivity Firewall. This is the interface filter that is selected on the System→WAN Interfaces→Edit IP Address screen. If no interface filter has been selected, the default of Deny All is used.

State

Enable

This WAN interface is currently enabled. An asterisk (*) means that the Interface Debug option on the WAN PPP Advanced Configuration screen is enabled.

Disable

This WAN interface is currently unavailable.

Actions

Configure

Click to configure a new IP address for the associated device, add or modify PPP advanced and authentication settings. The Configure WAN Interfaces screen appears.

Enable/Disable

Click to toggle between Enable (on) and Disable (off).

Statistics

Click to view Statistics for the interface.

WAN Statistics

This screen (System→WAN Statistics) provides counters that can help you diagnose and troubleshoot problems with your WAN interfaces. Fields on this screen are described in the following tables.

Figure 10 WAN Statistics screen

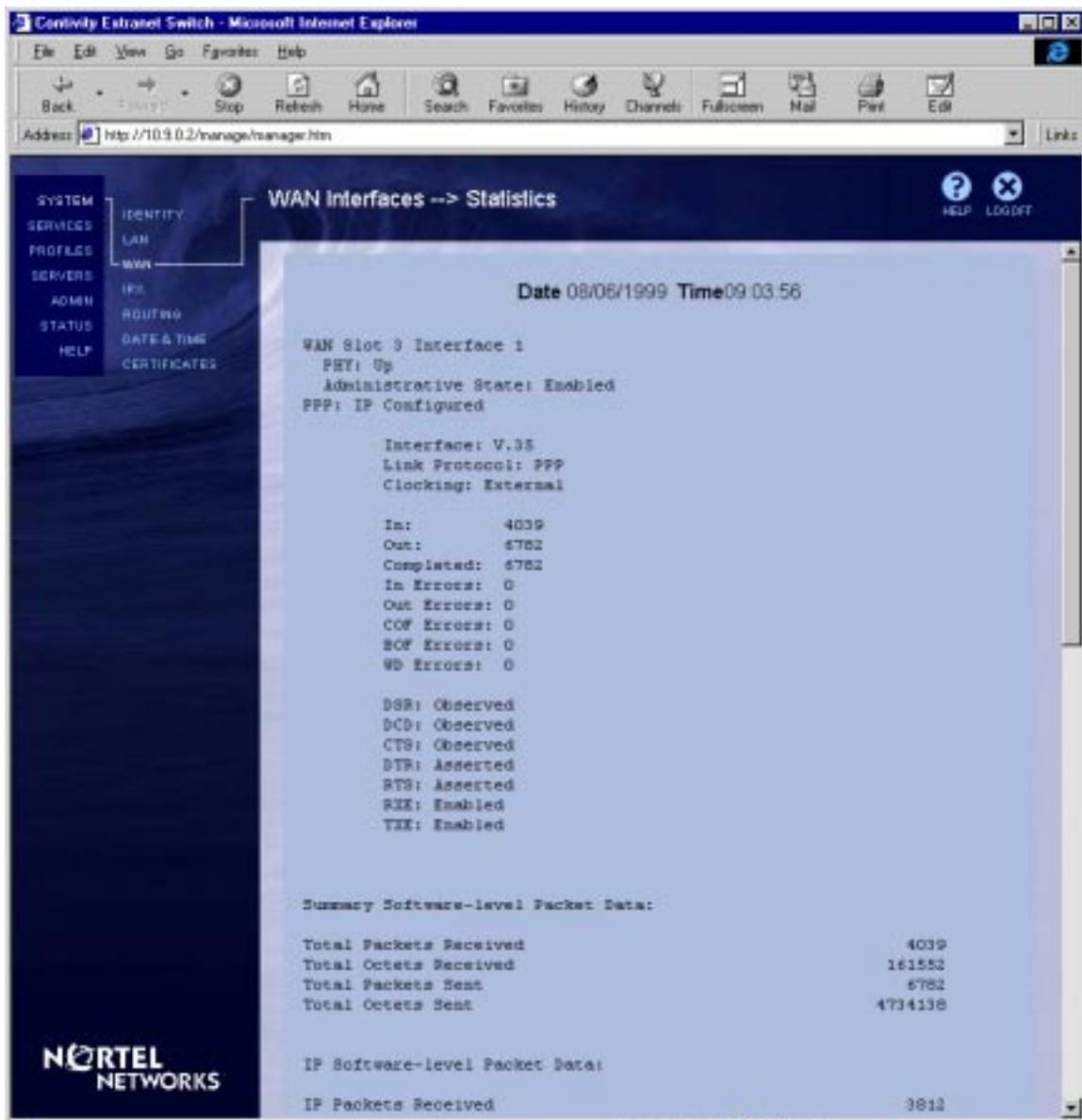


Table 3 WAN Statistics

Field	Description
WAN Slot 2 Interface 2	The slot and interface numbers
PHY	The state of the physical link is either up or down
Administrative State	The Administrative state is either enabled or disabled
PPP	The state of the Point-to-Point Protocol (PPP)
Interface	The physical interface type
Link Protocol	The link protocol type
Clocking	The switch relies on the channel service unit/digital service unit (CSU/DSU) to provide the signaling clock at the T1 physical level.
In	Packets received over this link
Out	Packets sent over this link
In Errors	Errors while receiving packets over this link
Out Errors	Errors while sending packets over this link
Cof Errors	Counter overflow errors
Bof Errors	Buffer overflow errors
WD Errors	Watchdog errors
DSR	Data set ready signal
DCD	Data carrier detect signal
CTS	Clear-to-send signal
RXE	Receive signal
TXE	Transmit signal

Table 4 Packet Data Statistics

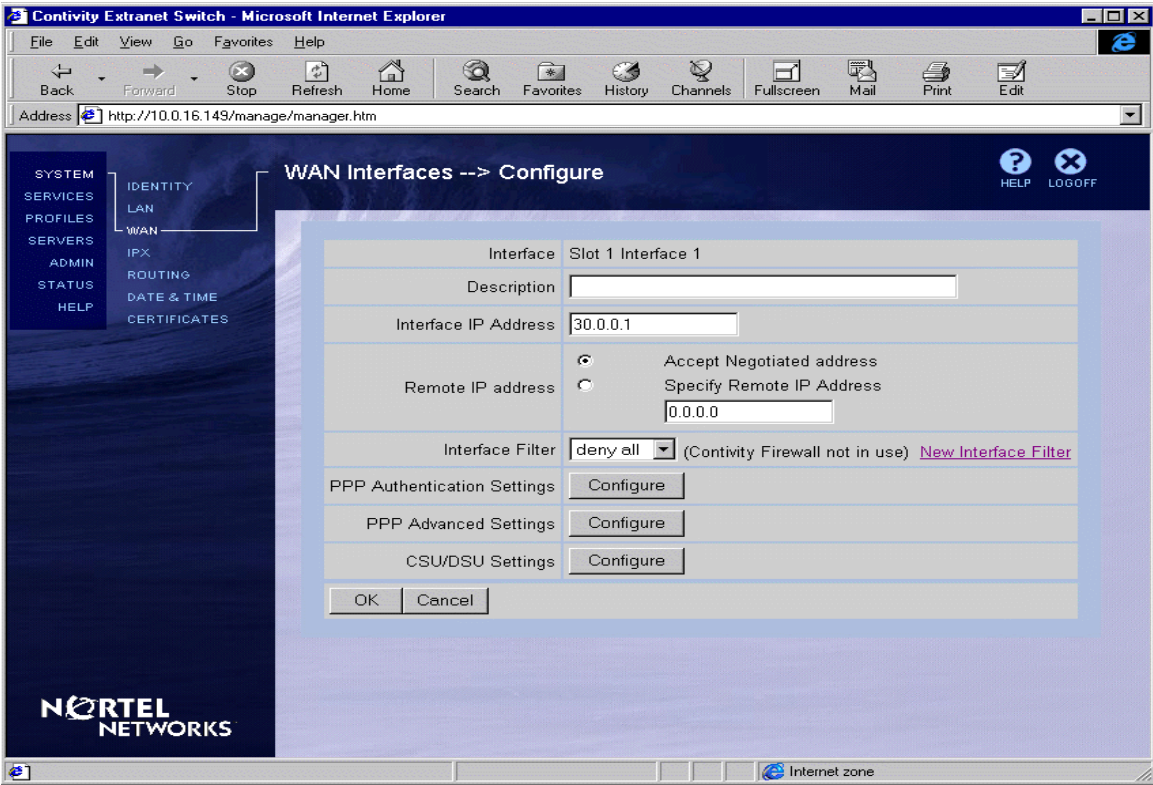
Software-Level Packet Data	Description
IP Fragments Received	IP fragments received
Routing Filter Drops	Routing filter drops occur when packets are filtered because no access rights are permitted to the resources specified by the designated filters.
IP Local System Filter Drops	Local system filter drops occur when packets are destined to the management interface but are dropped due to lack of authorization access.
IP Local Interface Filter Drops	Local interface filter drops occur when packets are destined to a physical interface but are dropped due to lack of authorization access.
IP PAT Drops	Public Address Table (PAT) drops pertain to the number of packets dropped prior to being authenticated and having a tunnel established on a public interface.
IP Header Error Drops	IP Header Error Drops occur whenever there is an error in the IP header.

Configure WAN Interface Settings

The Configure WAN Interface Settings screen (System→WAN Configure) allows you to configure WAN devices with local and remote IP addresses and PPP-related settings. When you click the PPP Authentication or Advanced Settings configuration buttons, the associated configuration screen appears. You also use this screen to specify the interface filter that is used for the optional Contivity Firewall on this interface.

The addresses set on this screen are used by the IP Control Protocol (IPCP), which communicates IP addresses to peer connections over PPP. Many of these values are provided to you by your Internet Service Provider (ISP).

Figure 11 Configure WAN Interface Settings screen



Interface

This is the type, slot number, and interface to which this IP address is assigned. The module slots on the back of the switch are labeled Slot 1 through Slot 4, from left to right. Slot 4 is not supported.

Description (Optional)

Provide a brief interface description. For example, a site, location, address, user name, or configuration tag. This can be helpful for network administrators working with the switch after it has been configured.

Interface IP Address

You must enter an Interface IP Address to allow IP traffic to pass over a PPP connection. This is the switch's IP address as seen from a Public network. This IP address is normally provided to you by the ISP. A sample Interface IP Address is 192.19.2.33.



Note: The interface IP address and the remote IP addresses must be different.

Remote IP Address

Accept Negotiated Address

This option informs the peer connection (for example, your Internet Service Provider) that you accept the IP Address that it assigns itself.

This checkbox is **Enabled** by default.

Specify Remote Address

Enter a Remote IP Address to allow IP traffic to pass over a PPP connection. This is the IP address of the router that is connected to the switch. This address is used if you do not check Accept Negotiated Address above. This IP address is normally negotiated between the switch and the ISP. A sample Remote IP Address is 192.19.2.30.



Note: The Remote and Local IP addresses must be different.

Interface Filter

Shows whether or not the Contivity Firewall is in use (this reflects the selection on the Services→Firewall screen).

This entry also shows the interface filter that is currently being used by the Contivity Firewall. Use the dropdown menu to show a list of all interface filters that have been set up on the switch (on the Profiles→Filters screen), and to select a different filter for the Contivity Firewall.



Note: If you change the interface filter setting, a message informs you that you must restart your switch before the new interface filter is used. If the Contivity Firewall is not enabled, the new selection has no effect.

Use the New Interface Filter link to go to the Profiles→Filters screen and create a new filter.

The default Interface Filter setting is Deny All.

PPP Authentication Settings

Click Configure to set PPP Authentication Settings, including Local PAP and CHAP User IDs and Passwords.

PPP Advanced Settings

Click Configure to set PPP Advanced Settings, including Link Control Protocol (LCP) and IP Control Protocol (IPCP) Settings.

CSU/DSU Settings

Click Configure to set the T-1 with an integrated CSU/DSU Settings, including extended super frame (ESF) framing parameters and adding fractional T-1 channels.

T-1 with Integrated CSU/DSU

You can configure your T-1 interface with an integrated CSU/DSU from the System→WAN screen or the serial interface. Following is a list of screens that either allow you to configure or view status for the T-1 interface with an integrated CSU/DSU:

- System→WAN
- System→WAN→Configure
- Admin→Health Check
- Status→Statistics→WAN Status

Newer T-1 services use extended super frame (ESF) framing, which uses out-of-band signaling. The configuration parameters with ESF are:

- Line framing is ESF.
- Line coding is B8ZS.
- HDLC polarity is normal.
- Performance report message value is determined by the T-1 service provider.

Older T-1 services use super frame (SF) framing, which uses in-band signaling. The configuration parameters with SF are:

- Line framing is SF.
- Line coding is AMI.
- HDLC polarity is inverted.
- Performance report message should be set to “none” as it has no effect in SF framing.

Because SF framing uses in-band signaling, the data can generate a false yellow alarm. These false yellow alarms can be eliminated by setting one fractional T-1 channel to “off.” If you have the option of using SF or ESF framing, Nortel Networks recommends ESF framing because it provides better diagnostics and does not generate false yellow alarms.

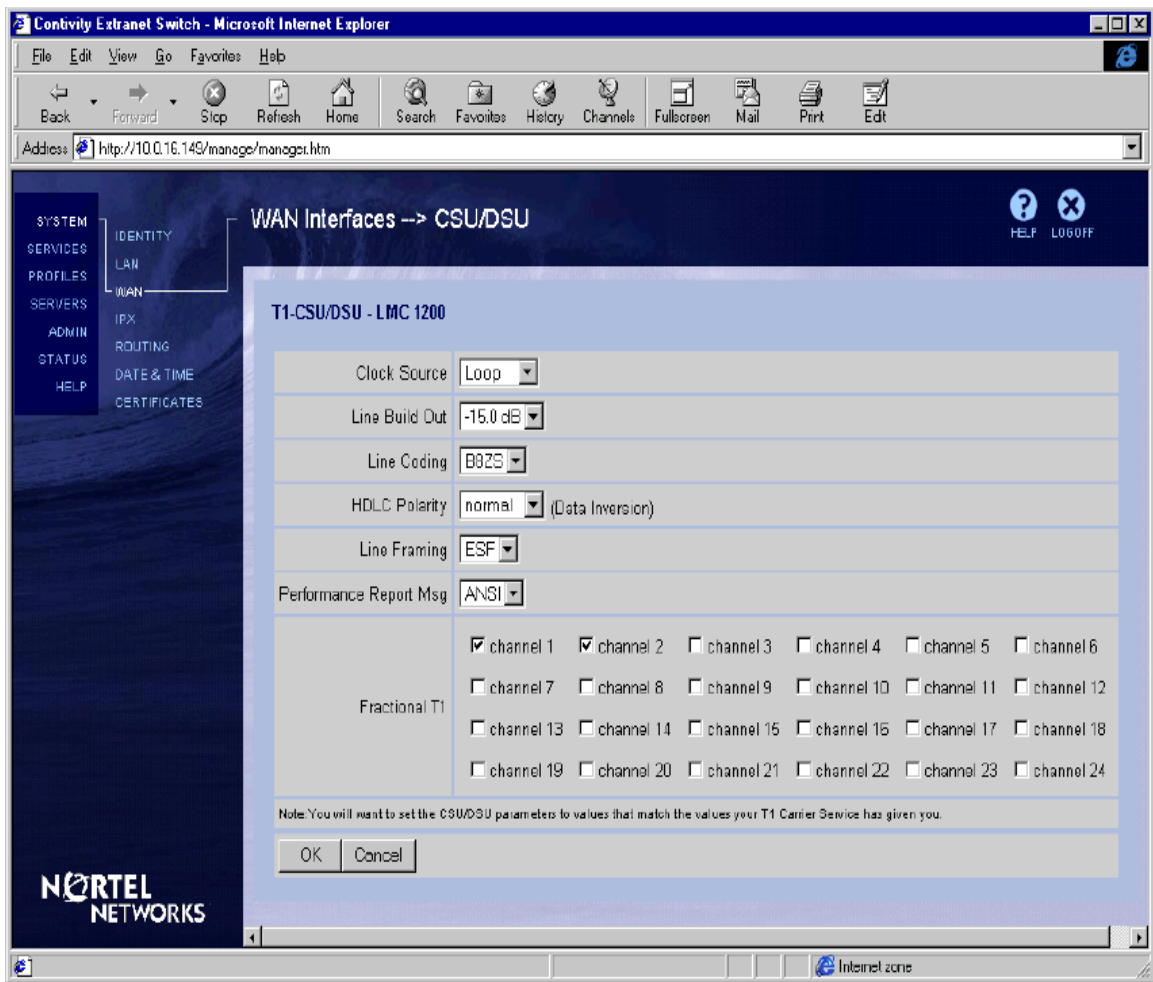
Initial configuration takes place when you install the card, and configuration changes are necessary when adding additional fractional T-1 channels.



Note: You must restart the switch after adding a T-1 card or after enabling a fractional T-1 line.

All of the CSU/DSU commands can be configured through the Web interface or the serial interface.

Figure 12 CSU/DSU



T1-CSU/DSU - LMC 1200

Clock Source

This field sets where the timing is being determined, from the switch (Internal) or from the T-1 service provider (Loop). The clock source is usually set to Loop when connected to a live T-1 service. Internal clocking is used for local or test applications only.

Line Build Out (dB)

The line build out value is a power level that is set based on the distance from the CSU/DSU to the T-1 service provider's switch. If the CSU/DSU card is close by, the switch requires less power and the line build out value is lower; if the card is far away, the switch requires more power and the line build out value is higher. This setting is determined by the T-1 service provider. Valid options are:

- 0.0
- -7.5
- -15.0
- -22.5

Line Coding

This field sets the method of encoding binary digits on the line. The line coding value is supplied by the T-1 service provider. Valid options are AMI and B8ZS.

HDLC Polarity

This field determines whether or not the user data is inverted. This field must be synchronized with the AMI line coding; otherwise, you might violate the AMI specification. Both the local and the remote CSU/DSU must terminate the T-1 data circuit with the same setting: either both using Normal or both using Inverted. Valid options are Normal and Inverted.

Line Framing

This field determines the low-level protocol between the T-1 service provider and the switch. It determines how the data is encapsulated and it handles the signaling for alarms and loopbacks. The newer ESF framing uses out-of-band signaling, while the older SF framing uses in-band signaling. The line framing value is supplied by the T-1 service provider. Valid options are SF and ESF.

Performance Report Mesg

The Performance Report Message parameter is a part of the ANSI T-1 specification. It generates messages that state how many errors there are per second. This value is used with ESF framing only. When using SF framing, this parameter has no effect but should be set to None to avoid any confusion. The Performance Report Message value is supplied by the T-1 service provider and are None and ANSI.

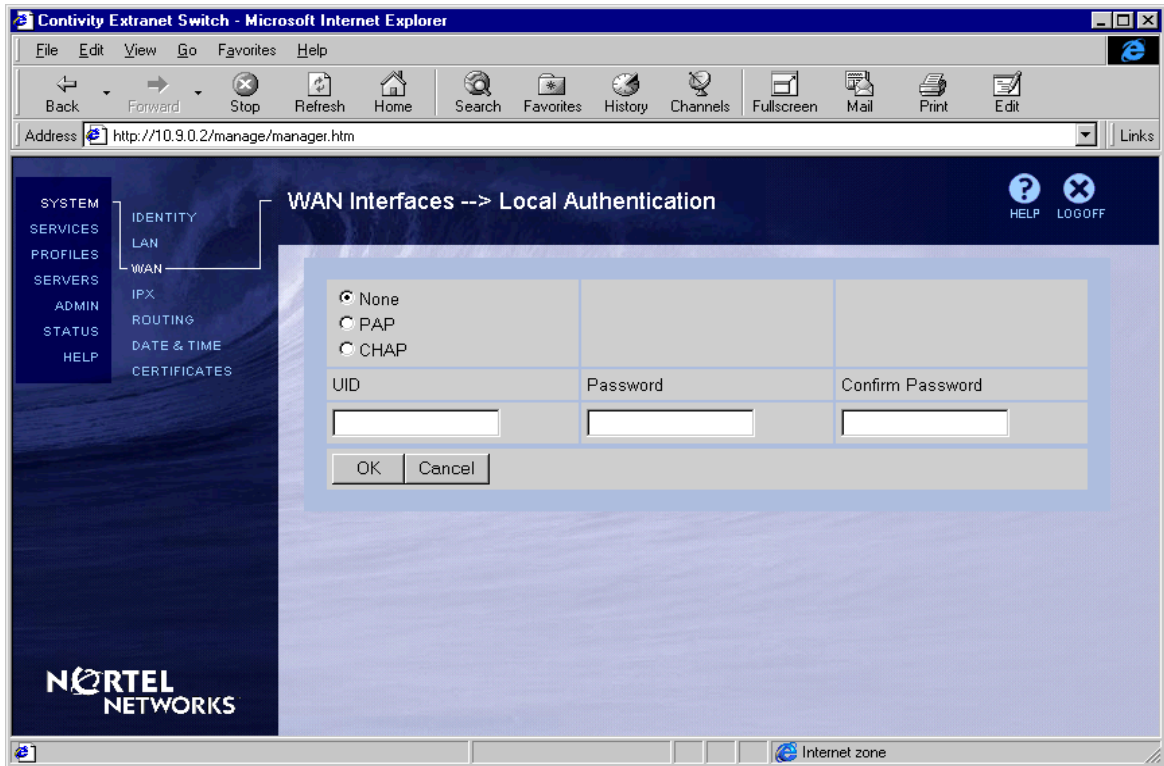
Fractional T-1

A T-1 service consists of up to 24 channels. Typically, you purchase the number of necessary channels from the service provider, and you can add additional channels (up to 24) as growth requires. When you add a fractional T-1 channel, you must enable it through this parameter and restart the system. Valid options for each of the 24 DS-0 channels are On (checked) and Off (unchecked).

Local Authentication

The WAN Interfaces Local Authentication screen (System→WAN Configure PPP Authentication) allows you to configure Local Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) User IDs and Passwords, and other details.

The ISP providing the WAN connection to the switch might require a user ID and password. Select the appropriate authentication method, PAP or CHAP, as required by the ISP. If authentication is not required, then select None.

Figure 13 Local Authentication

None

Click None (default) to allow a connection without authentication on this interface.

PAP

Click to enable the Password Authentication Protocol (PAP). PAP is a simple method for a peer (the switch) to establish its identity during link setup. After establishing the identity, the ID and Password are transmitted repeatedly by the peer until the server acknowledges authentication or the connection is ended.

PAP is a lightweight authentication method, and the passwords are transmitted in clear text form (not encrypted). This leaves open the possibility for someone to trace the PPP setup and learn the WAN interface UID and passwords.

Most administrators do not consider the link setup as a possible security issue, and most ISPs use the link authentication described here for accounting purposes.

The PAP User ID and Password are used by the switch to authenticate with the service provider's T1 connection. They are provided to you by your ISP.

CHAP

Click to enable the Challenge Handshake Authentication Protocol (CHAP), which is the default setting.

CHAP uses a handshake to verify the identity of a peer. During link setup, the server (authenticator or ISP) sends a challenge message to the peer (the switch). CHAP depends on a “secret” that is known only by the server and the peer. The peer responds with a calculated value based on the secret. The server matches the calculated value against its own calculation. If the values match, the peer is successfully authenticated.

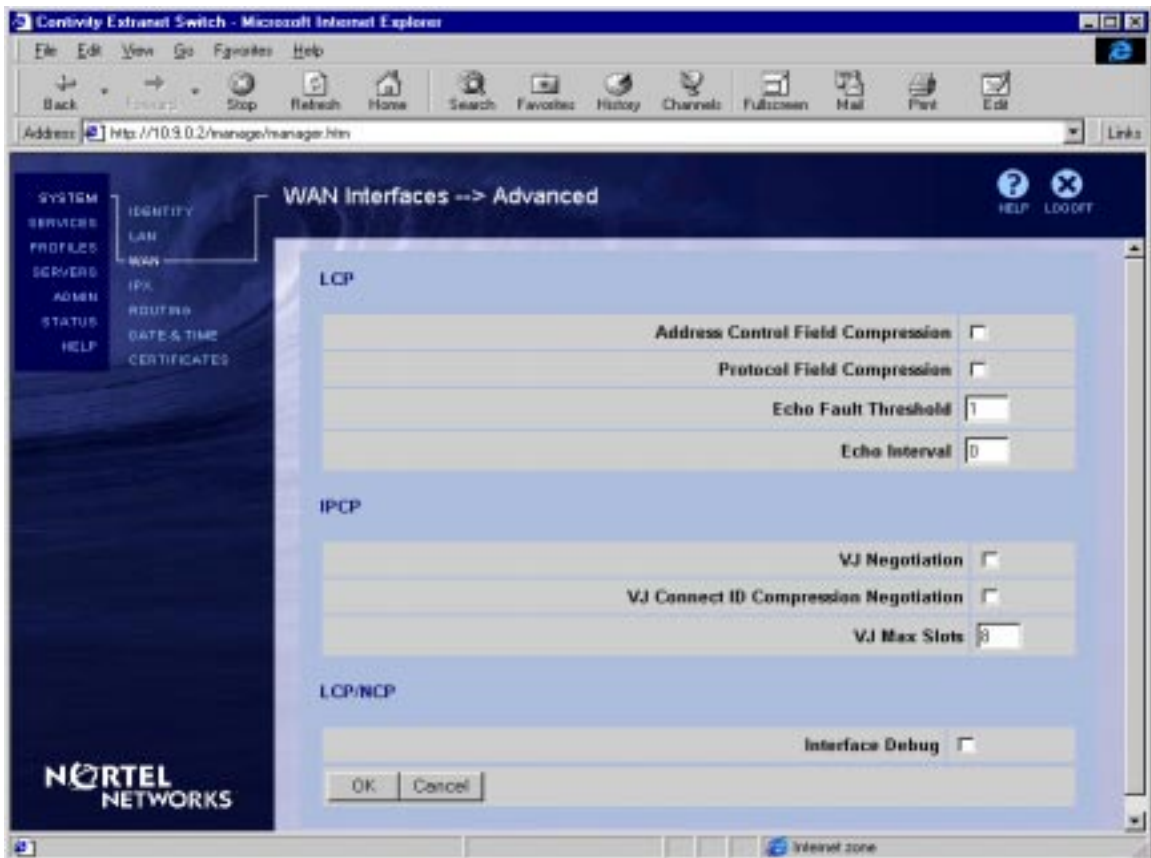
CHAP is a stronger authentication method than PAP. The clear-text secret is never transmitted over the communications link. Therefore, a trace of the session would not reveal the passwords.

The CHAP User ID and Password you assign are used by the switch to authenticate with the service provider's T1 connection. They are provided to you by your ISP.

WAN Interface Advanced Settings

The WAN Interface Advanced Settings screen (System→WAN Configure PPP Advanced) allows you to configure various connection options between the ISP and the switch, and to specify certain dial-up networking attributes, including Link Control Protocol (LCP) and IP Control Protocol (IPCP) Settings.

Figure 14 WAN Interface Advanced Settings



LCP Settings

The Link Control Protocol (LCP) session negotiates various link options between the switch and the ISP.

Address Control Field Compression

Click to enable Address Control Field Compression, which then compresses the Address Control Field and reduces packet overhead by one byte. Address Control Field compression is Disabled by default.

Protocol Field Compression

Click to enable Protocol Field Compression, which then compresses the Protocol Field and reduces packet overhead by one byte. Protocol Field Compression is disabled by default.

Echo Fault Threshold

You can set the number of times LCP attempts an Echo request without receiving a reply. The link is dropped when the number of echo requests exceeds the number in the Echo Fault Threshold box.

The possible range is 0 to 255 (0 indicates disabled); default is 1.

Echo Interval

You can set the Echo request Interval in seconds. Use this interval along with the value of the Echo Fault Threshold box to determine if a link has been disconnected.

The possible range is 0 to 255; default is 0 (Disabled).

IPCP Settings

The IP Control Protocol (IPCP) settings allow you to specify certain dial-up networking attributes. Typically, IPCP handles address assignment and configuration of domain name system (DNS) or windows Internet naming service (WINS) server settings.

The switch allows you to manipulate header compression options that can help optimize data transfers between systems.

VJ Negotiation

Click to enable Van Jacobson (VJ) Compression Negotiation. VJ Compression compresses the TCP/IP header fields on a per TCP/IP flow basis and reduces packet overhead. VJ Negotiation is disabled by default.

VJ Connect ID Compression Negotiation

Click to enable Van Jacobson (VJ) Connect ID Compression, which then further reduces the VJ compression header and increases packet transmission performance. This option is used only when a single TCP/IP flow is active at any single time over the link. VJ-style TCP/IP header compression identification is **Disabled** by default.

VJ Max Slots

This is the Maximum number of concurrent VJ-compressed TCP/IP flows. The range is from 2 to 16; default is 8.

LCP/NCP

Interface Debug

This option, under the Link Control Protocol/Network Control Protocol, sends PPP control packets to the Event log. This is a Nortel Networks internal Customer Support utility that helps diagnose and troubleshoot WAN interface problems.

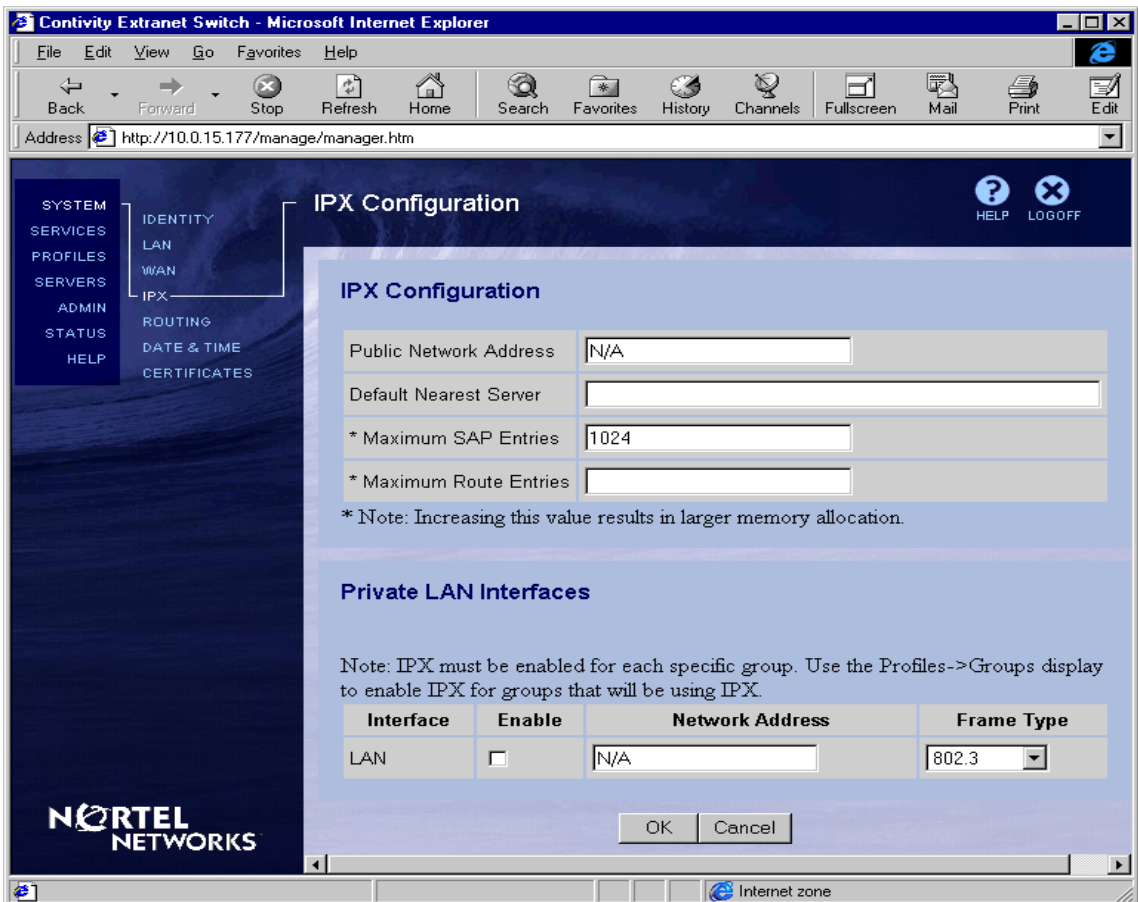
IPX (Internetwork Packet Exchange)

The Internetwork Packet Exchange (IPX) protocol is the Novell adaptation of the Xerox Networking System (XNS) protocol.

IPX Configuration

Click System→IPX to configure IPX support.

Figure 15 System→IPX Configuration



Public Network Address

Enter the IPX Public Network Address. This is the network address that is assigned to clients tunneling into the switch. The Public Network Address is a 4-byte hexadecimal number that must be unique (it cannot match any other IPX network address). A sample Public Network Address is 4F1A3BC2.

The Public Network Address also consists of a node address that is dynamically assigned by the switch to each tunneled-in client system. The Node Address is a randomly allocated number that cannot be overwritten or changed in any way.



Note: Leaving the Public Network Address blank disables IPX on the switch.



Caution: You must restart the system from the Admin→Shutdown screen for Public Network Address changes to take effect.

Default Nearest Server

Enter the name of the server that you want to be the Default Nearest Server. The Default Nearest Server name can consist of up to 48 ASCII characters. When a remote system establishes an IPX connection with the switch, the system sends a Get Nearest Server packet to the switch. In response to a Get Nearest Server request, the switch returns the name and IPX address of the server specified here. This assumes that the server is available; otherwise, the switch returns the name and IPX address of the server that is topologically closest to the requesting system.

Maximum SAP Entries

Shows the largest number of SAP (Service Advertising Protocol) entries that the switch handles concurrently. SAP is a Novell protocol that provides a means for servers to advertise their services to routers, switches, and other servers.

Each SAP entry that you allocate requires about 100 bytes of memory (10,000 entries requires about 1 MB of memory). Therefore, you should keep the number of entries slightly greater than the number of servers that you support to allow for future growth. The default value is 1024 entries; the range is from 10 to 10,000 entries.

Maximum Route Entries

Shows the largest number of IPX route entries that the switch handles concurrently. A route entry is required for each reachable IPX network that is learned through the IPX RIP protocol.

Each route entry that you allocate requires about 100 bytes of memory (10,000 entries requires about 1 MB of memory). Therefore, you should keep the number of entries slightly greater than the number of routes that you support to allow for future growth. The default value is 1024 entries; the range is from 10 to 10,000 entries.

Private LAN Interfaces

Interface

LAN represents the Ethernet interface on the system board, which is installed on every switch.

Slot *n* Interface *n* represents an optional local or wide area network card in expansion Slot *n* using Interface *n*.

Enable

Click to enable the interface for IPX support.

Network Address

Enter the IPX interface Network Address. The IPX Network Address that you configure on this interface must be the IPX Network Address of the LAN.

Frame Type

Click the drop-down list box to select an IPX Frame Type. The IPX Frame Type that you select on this interface must be the IPX Frame Type being used on the LAN.

The switch can forward the following IPX packet types:

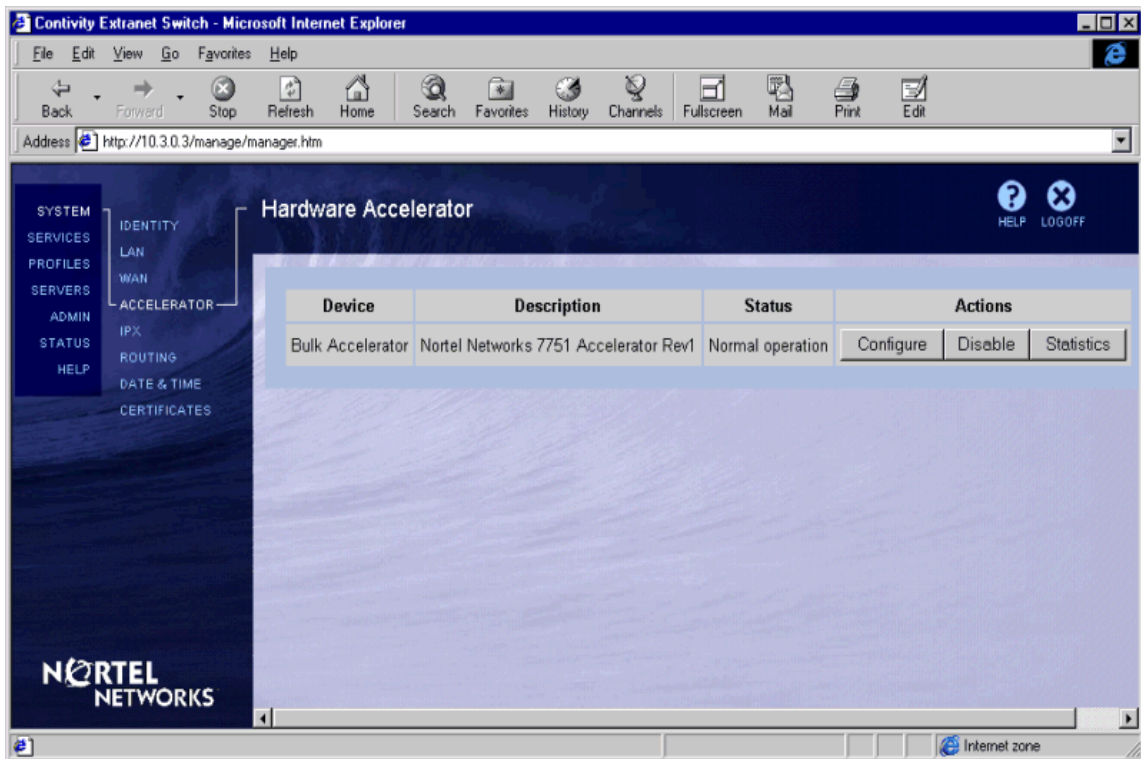
- 802.3 (Raw) refers to 802.3 framing without the 802.2 link layer control (LLC).
- 802.2 frame includes 802.3 and 802.2 logical link control (LLC) frames.
- SNAP Sub Network Access Protocol (SNAP) is like 802.2 with expanded link layer control (LLC) capabilities.

- Ethernet II frame type is also similar to 802.2, yet it has a type field rather than a length field. It does not use a link layer control (LLC) header in its data field.

Hardware Encryption Accelerator

The hardware accelerator screen shows the operational status that the switch reports on the hardware accelerator card and allows you to enable automatic recovery in case the card stops running. When the switch detects a recoverable failure, all sessions fail-over and are then handled by the software until the hardware resets and comes back on line.

Figure 16 Hardware Accelerator



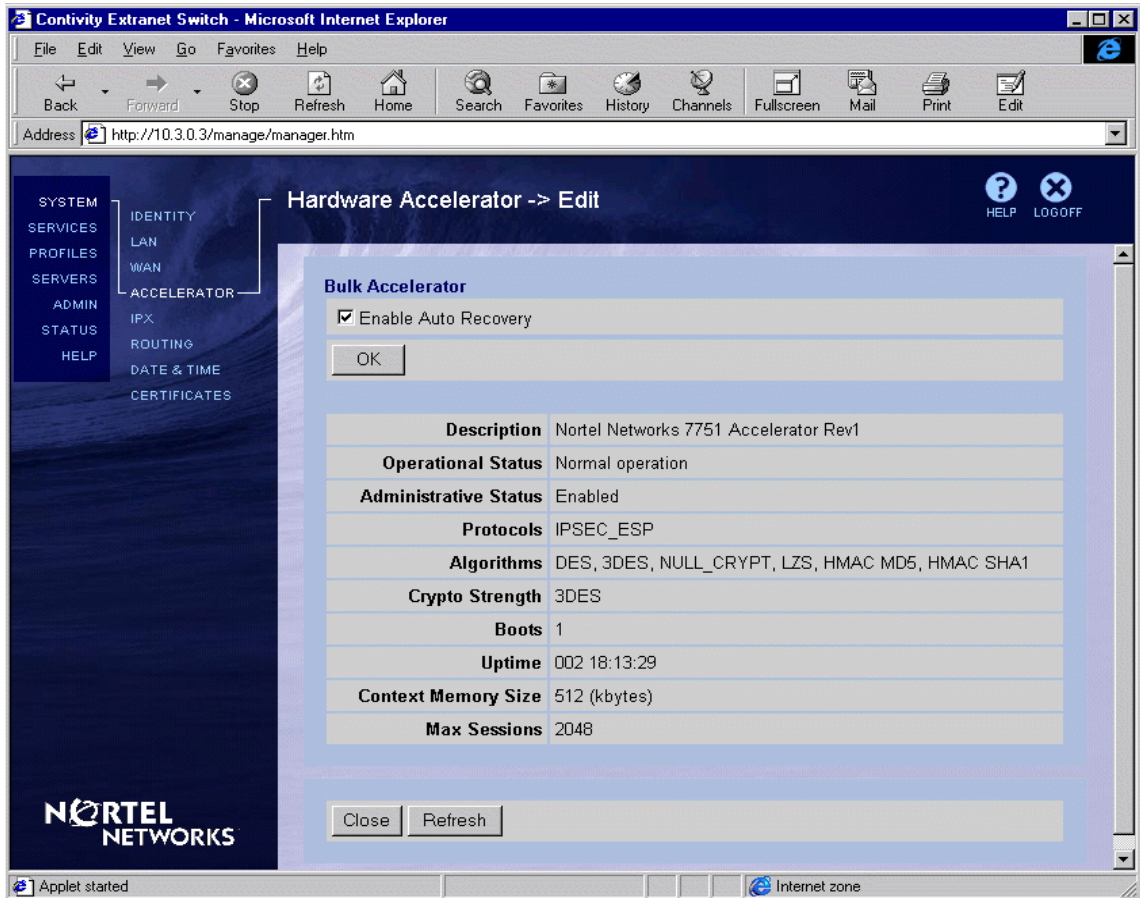
You must have Administrator privileges to configure the card, and you must restart the switch after configuring it.

The accelerator supports a maximum of 1024 tunnels. A tunnel consists of two sessions, one each for incoming and outgoing traffic. Each session comprises a set of logical characteristics and parameters that are associated with a single communication path in a tunnel that renders a full-duplex connection. Thus, the number of tunnels supported by an accelerator is exactly half the maximum session count.

Following is a listing of the switch's configuration, status, and monitoring paths related to the hardware accelerator:

- System →Accelerator→Hardware Accelerator: Configure
- Status→Health Check
- Status→Statistics→Hw Accel Stats
- Status→Statistics→Hw Accel Info
- Status→Event Log

The Hardware Accelerator screen shows the operational status that the switch reports for the card.

Figure 17 Hardware Accelerator Configuration

Bulk Accelerator

Auto Recovery Enabled

This selection gives the operator control of what happens when if the card fails and the failure is recoverable. When enabled, the card automatically resets and restarts, when a recoverable failure is encountered.

Auto Recovery is the only configurable parameter. By default it is enabled and it maintains this state through a restart

Description

A description of the device vendor, device type, and serial number (if applicable).

Operational Status

Status can be viewed on the Status→Health Check and the Status→Statistics: HwAccelInfo screens. The operational status can be:

- Disabled means that the card is disabled.
- Active means that the card is attached and is active.
- Shutdown means that in this state you can manually reenable the card after a recoverable failure has been detected (when Auto Recovery Enabled is Off).
- Failed means that the card is not operating properly. Contact Nortel Networks Customer Support for additional information.

Administrative States

The card is either Enabled or Disabled. It is enabled by default.



Note: You can disable the card at any time, even when it is processing tunnel traffic. In this case, the tunnels are processed in software. When the card is subsequently enabled, any tunnels that had been running on the hardware when it was disabled, revert to running on the hardware.

Protocols

Shows the protocol running on the card: IPSEC_ESP.

Algorithms

Shows the encryption and authentication protocols that the card supports:

- DES Data Encryption Standard
- 3DES Triple Data Encryption Standard
- NULL_CRYPT – IPSec ESP authentication and compression only; encryption is turned off. You can use this setting as a troubleshooting mechanism.

- LZS – Lempel/Ziv/Stac, which is a de facto standard for IPSec compression.
- HMAC MD5 – Header Message Authentication Code with Message Digest, which provides integrity that detects packet modifications.
- HMAC SHA – Header Message Authentication Code Secure Hash Algorithm, which produces a 160-bit hash. SHA is regarded by cryptographers as being more resistant to attacks than MD5. It does not encrypt data.

Crypto Strength

Shows the available cryptographic strength, which is either 3DES (triple DES) or DES, depending upon the maximum key length.

Boots

Shows the number of times the card has been restarted.

Uptime

Shows the current duration that the switch has been running (days:hours:minutes:seconds).

Context Memory Size

Shows the amount of context memory on the card: 512 kbytes.

Max Sessions

Shows the maximum number of sessions. When you divide this number by two you get the number of tunnels (2048 sessions represents 1028 tunnels).

POST Results

Shows the passing and failure indications for each power-on self test (POST) type. This field displays when there is a POST failure only.

Statistics

You can view statistics for the hardware accelerator on the Status→Statistics HwAccelCounters screen. Byte counters are all 64-bit integers:

- Total packets on egress
- Total bytes on egress
- Total packets on ingress
- Total bytes on ingress
- Corrupt bytes (see explanation)
- Corrupt packets
- Expanded bytes (see explanation)
- Expanded packets

Corrupt bytes and packets counts reflect packets that were not processed because they were corrupted in transit. Indications of a corrupt packet include: no LZS end marker, mismatch MAC.

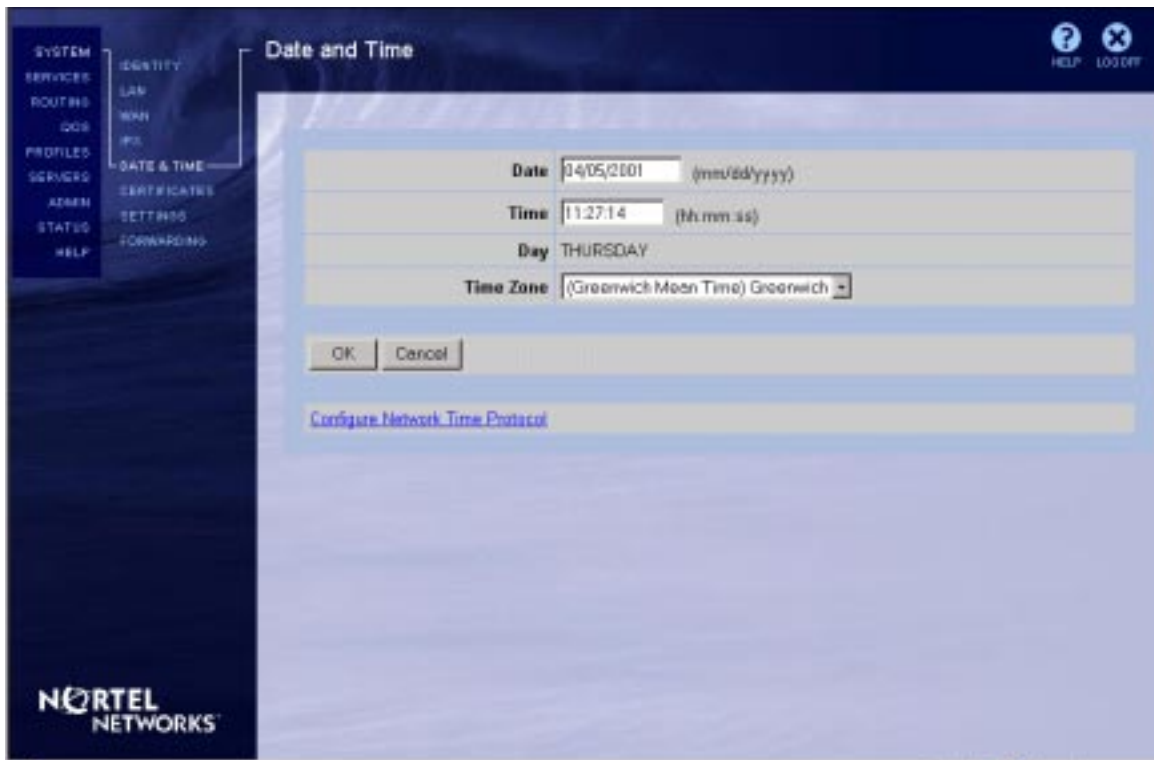
Expanded bytes and packets counts reflect packets that expanded when compressed by the LZS algorithm. These counters are important because they indicate a heavier load on the accelerator since packets which expand must be sent a second time to the accelerator with compression disabled. If there are many sessions transporting incompressible traffic (such as a video stream), the overall performance of the switch is degraded relative to its performance when all sessions carry compressible data (such as FTP or text files).

Most of these statistics are maintained for debugging and tuning purposes.

Date and Time

This screen shows the current Date, Time, and Day of the week for the switch. You can change the time based on your time zone, or make daylight savings time adjustments, as necessary.

To change either the Date or Time values, select the fields and enter the new values.

Figure 18 Date and Time

Date

Shows the current month, day, and year (mm/dd/yyyy).

Time

Shows the current hour, minute, and seconds (hh:mm:ss) as displayed by a 24-hour clock (00:00:00 to 23:59:59).

Day

Shows the current day of the week. The day is based on the month, date, and year, and it cannot be changed manually.

Time Zone

Click the drop-down list box to select the appropriate time zone. Time zones can be a critical factor in the usage of digital certificates.

Configure Network Time Protocol (NTP)

The System→Date and Time→Network Time Protocol screen allows you to set up the Network Time Protocol (NTP) on the switch. NTP synchronizes the clocks of various devices across networks. It also automatically adjusts the time of network devices so that they are synchronized within milliseconds. The switch receives NTP updates from an NTP time server and continuously synchronizes its clock to universal standard time. The switch supports up to eight NTP (unicast) servers and broadcast, multicast servers.

Figure 19 Network Time Protocol

The screenshot shows a web interface for configuring the Network Time Protocol (NTP). On the left is a dark blue sidebar with a menu containing: SYSTEM, SERVICES, ROUTING, QOS, PROFILES, SERVERS, ADMIN, STATUS, and HELP. A sub-menu is open under 'SYSTEM', showing: IDENTITY, LAN, WAN, IPX, DATE & TIME (which is highlighted), CERTIFICATES, and SETTINGS. The main content area has a title bar 'Network Time Protocol' with 'HELP' and 'LOGOFF' icons on the right. The configuration options include: an 'Enable' checkbox, a 'Synchronize time with Broadcast Server' checkbox, and a 'Synchronize time with Multicast Server' checkbox. Below these are two sections: 'Servers' and 'Trusted Keys'. Each section contains the text 'There are no servers in the database.' and 'There are no trusted keys in the database.' respectively, followed by an 'Add' button. At the bottom are 'OK' and 'Cancel' buttons, and a link that says 'Return to the Date and Time page'.

Check the Enable NTP check box to enable NTP on the switch.

If you want the switch to listen for and respond to broadcast messages, check the Synchronize time with NTP Broadcast Server box. If you want the switch to listen for and respond to multicast messages, check the Synchronize time with NTP Multicast Server box. The IP multicast address is 224.0.1.1 for NTP.

NTP listens for both broadcast and multicast messages at the group address of the global network. To avoid disruption in multicast mode, both the client and servers should use authentication and the same trusted key and key identifier.

Servers

The switch lists any existing NTP servers.

Server IP Address

IP address of the NTP (unicast) server.

Interface

For security, you can specify either a Private or Public interface. The private interface is the management IP address. When adding a public interface, you can choose from a list of public interfaces. If you are using the Contivity Firewall, you need to configure an interface filter to add NTP.

Key ID

Specifies the Key ID for Message Digest (MD5) authentication. In authentication mode, each packet transmitted has a 32-bit Key ID and a 64/128-bit cryptographic checksum using MD5 algorithms. With MD5, the receiving peer recomputes the checksum and compares it with the one in the packet. They must share at least one MD5 key (trusted key) and must associate the shared key with the same Key ID.

Bursting

Specifies to send a burst of eight packets at each poll interval.

Version

NTP version number (1, 2, 3, or 4) used on the NTP server. The default is 3.

Actions

Edit

To edit an existing NTP server, click on the edit button in the Action column.

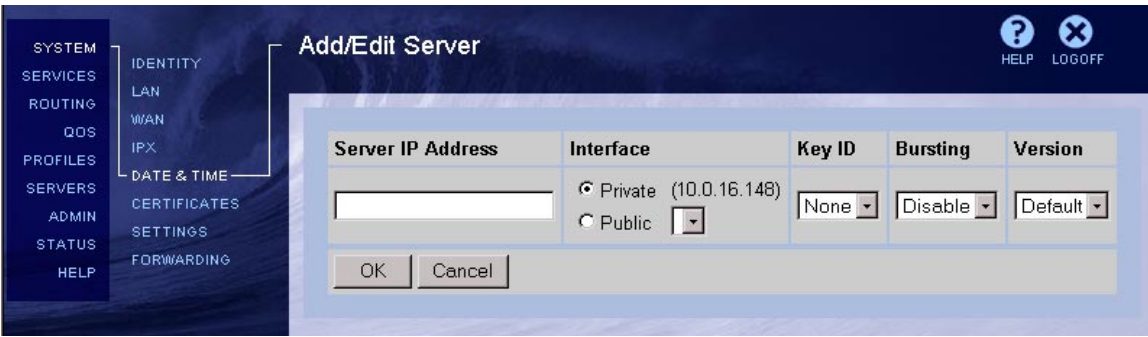
Delete

Click on the Delete button to delete an NTP server.

Add

You can add an NTP server by clicking on the Add button. The switch displays the Add/Edit Server screen. If you are adding an NTP server, enter the appropriate information as described above.

Figure 20 Add/Edit NTP server screen



Trusted Keys

Key ID

Specifies the Key ID for MD5 authentication.

Actions

Edit

To edit an existing key ID, click on the edit button in the Action column.

Delete

Click on the Delete button to delete the trusted key.

Add

You can edit an existing area key ID by clicking on the Edit button. The switch displays the Add/Edit Trusted Key screen. Enter the key Id, the password and the password confirmation.

Click on the Return to the Date and Time page link to return to the previous page.

Certificates screen

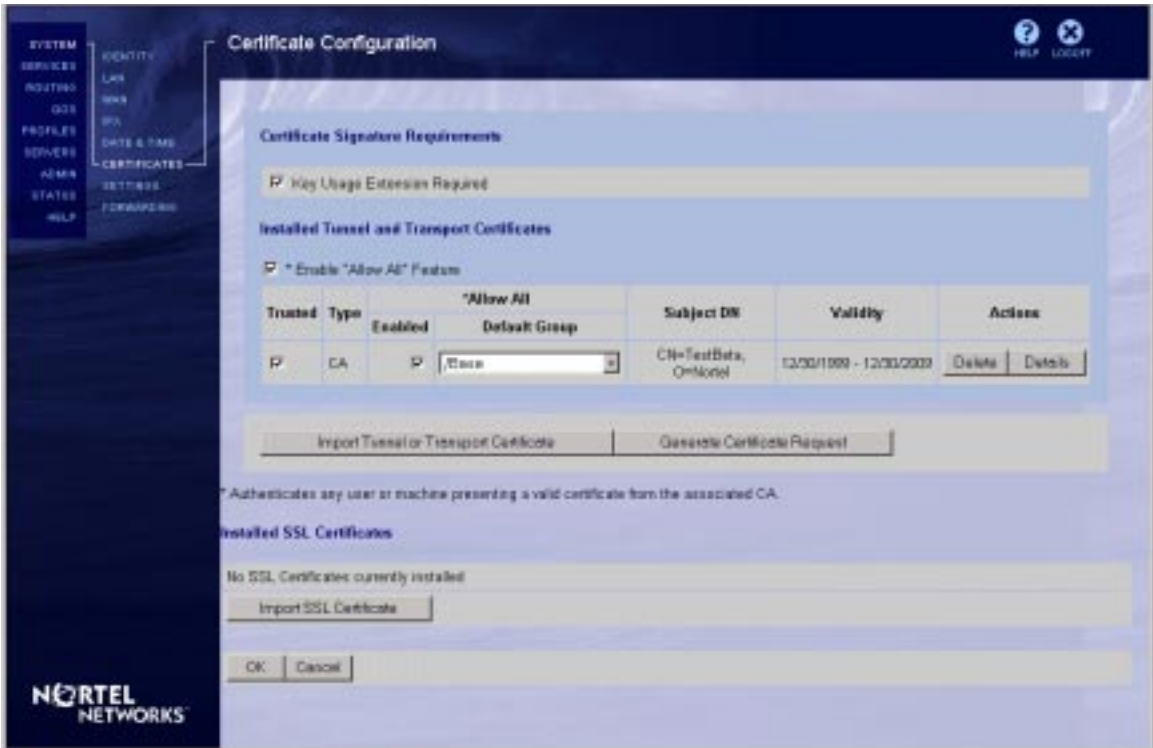
This screen allows you to import both tunnel and SSL certificates to the switch and generate a certificate request for a server tunnel certificate. When you have added certificates to the switch, it shows the available certificates. Tunnel Certificates are used to authenticate IPSec tunnel connections. SSL Certificates are used to secure connections with LDAP servers.

A Certificate is an electronic “document” that identifies an entity such as a Certification Authority. You should trust a certificate only if you trust the person or organization that issued it (an approved Certificate Authority).

Key Usage Extensions Required

Enable this option to require key usage extensions to be present in certificates that are presented via a tunnel request. This option is enabled by default.

Figure 21 Installed Certificates



Enable Allow All Feature

Click the Enable button to allow all clients attempting to authenticate against a CA Certificate, without an explicit user entry, the ability to do so.



Note: Branch Office connections do not support the CA Certificate Allow All feature. Therefore, you must configure an explicit Branch Office connection.

Trusted

Check to designate this certificate as Trusted (you have previously verified that this certificate is authorized and has been validated).

Type

Shows the certificate type, whether it is a Certificate Authority (CA) or a Server Certificate.

Allow All

The Allow All feature must be Enabled for each CA Certificate against which you want to permit authentication without an explicit user entry. This allows anyone with a valid certificate from the particular CA to establish a tunnel connection.

Also, you must associate a Default Group with that certificate. The client authenticating with the Allow All feature then uses the attributes associated with that group.

Subject DN (Distinguished Name)

Shows the certificates Subject Distinguished Name components; for example, Common Name, Organizational Unit, Organization, and Country.

Validity

Shows the dates through which the certificate is valid (for example, 01/29/98 to 01/29/99).

Actions

Delete

Click to Delete the selected certificate. A delete confirmation dialog box then asks you to confirm the deletion.

Details

Click to view the specific details of the Certificate owner and issuer. This screen also shows the certificate's fingerprint, which is important in verifying the authenticity of a CA certificate, especially when first imported.

Import Tunnel Certificate

Click to display the PKCS certificate import screen. When importing a PKCS#7 encoded certificate, verify the fingerprint of the resulting imported certificate with the fingerprint supplied from the CA. It is important to obtain the fingerprint through some out-of-band mechanism (phone, postal mail, and so forth) to guarantee the supplied certificate is genuine.

Generate Certificate Request

Click to display the Create New Key and Certificate Request screen, which allows you to create a key and a certificate request.

Import SSL Certificate

Click to display the certificate import screen. When importing a PKCS#7 encoded certificate, verify the fingerprint of the resulting imported certificate with the fingerprint supplied from the CA. It is important to obtain the fingerprint through some out-of-band mechanism (phone, postal mail, and so forth) to guarantee the supplied certificate is genuine.

Create New Key and Certificate Request

The Create New Key and Certificate Request screen allows you to provide the necessary X.500 Distinguished Name information for the switch requesting a certificate.

Figure 22 Create New Key and Certificate Request

Contivity Extranet Switch - Microsoft Internet Explorer

File Edit View Go Favorites Help

Address <http://10.0.16.148/manage/manager.htm>

Certificate Configuration

SYSTEM
SERVICES
PROFILES
SERVERS
ADMIN
STATUS
HELP
IDENTITY
LAN
WAN
IPX
ROUTING
DATE & TIME
CERTIFICATES

Create New Key and Certificate Request

Common Name (e.g. Entrust Reference #)

Organizational Unit (e.g. Finance)

Organization (e.g. ACME Networks)

Locality (e.g. Norfolk County)

State/Province (e.g. MA)

Country (e.g. US)

Public Key Size

OK Cancel

NORTEL NETWORKS

Internet zone

Create New Key and Certificate Request

Common Name

Enter the Common Name with which the switch is associated. For an Entrust PKI environment, this must be a valid Entrust Reference Number.

Organizational Unit

Enter the Organizational Unit with which the switch is associated.

Organization

Enter the Organization with which the switch is associated.

Locality

Enter the Locality in which the switch resides.

State/Province

Enter the State/Province in which the switch resides.

Country

Enter the Country in which the switch resides.

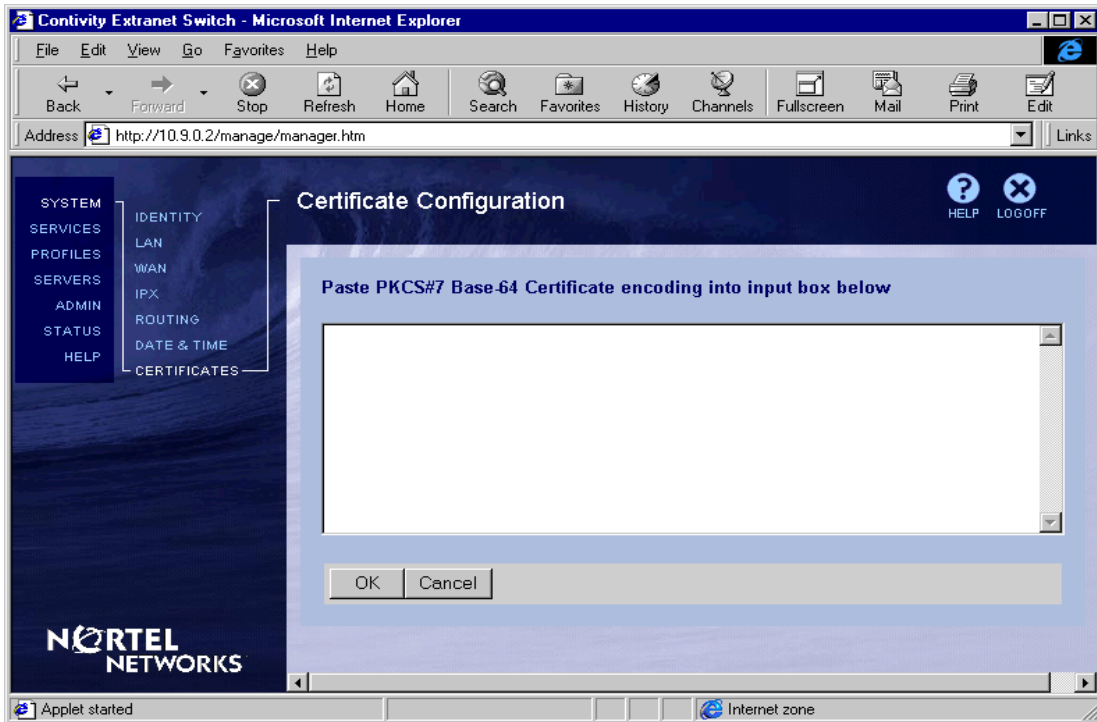
Public Key Size

Click the drop-down list to select one of the following exportable Public Key Sizes in bits (generally, larger keys are more secure):

- 512
- 768
- 1024
- 2048 (US only)

PKCS #10-Encoded Certificate Request

The Generate Certificate Request button returns the following sample PKCS (Public Key Cryptography Standard) #10-encoded Certificate request. Copy the contents of the certificate request into your Web browser's copy buffer. Submit the request to the applicable CA by pasting the encoding into the CA's request screen, following the instructions provided by the CA.

Figure 24 Paste PKCS #7 Base-64 Certificate

Server Certificate

Click Server Certificate to indicate you are importing a Server Certificate. Importation of a Server Certificate must correspond to a previous Server Certificate request.

Trusted CA Certificate

Click Trusted CA Certificate to indicate you are importing a Trusted CA Certificate.

Pasting a PKCS #7 Certificate

Copy the Public Key Cryptography Standard (PKCS) #7 ASCII text that is returned by the Create New Key and Certificate Request into the dialog box. Typically, a Certificate Authority provides this text to you.

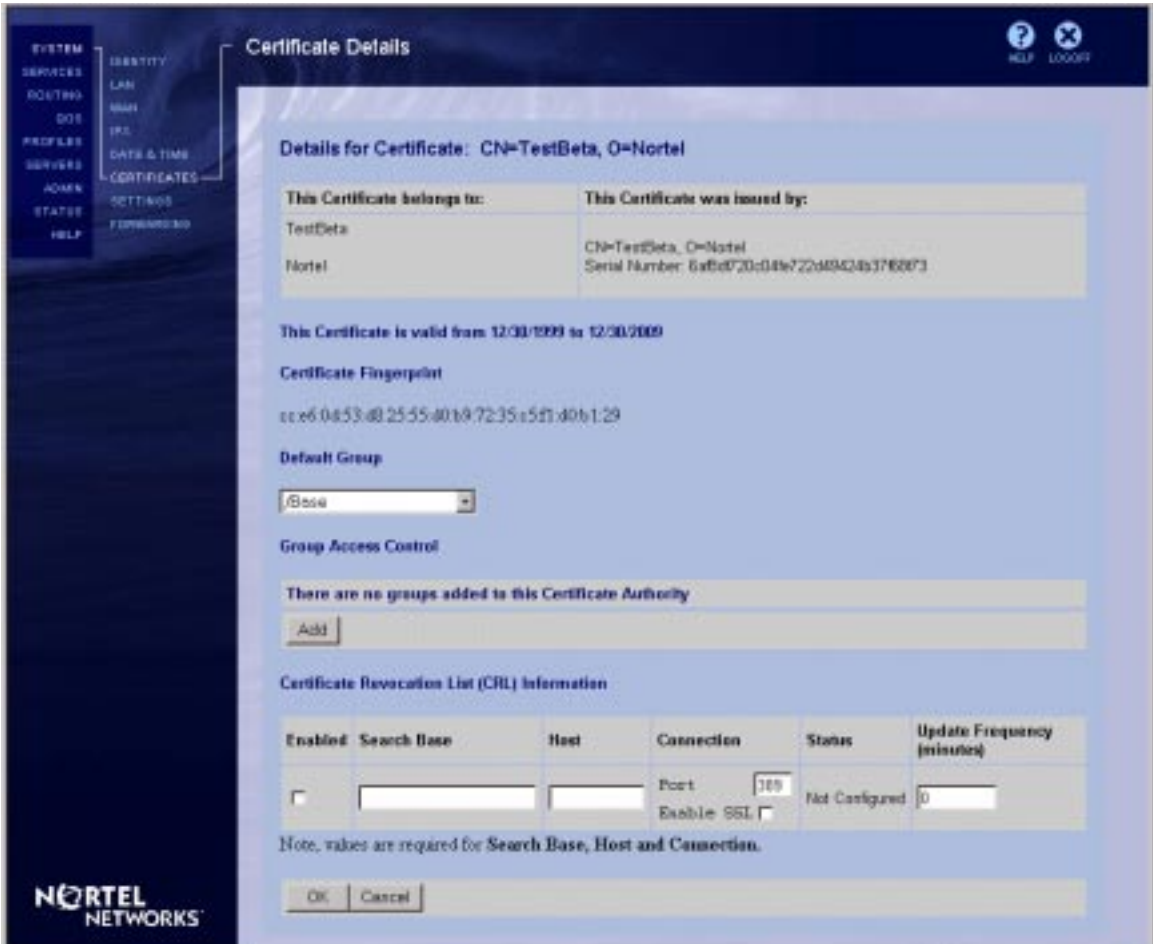
OK

Click OK to generate a certificate and store it on the switch.

Certificate Details

This screen provides the certificate details, including the owner of the certificate and who issued the certificate. Additionally, this screen provides the validity dates, the certificate fingerprint and, if a CA Certificate, the certificate revocation list details.

Figure 25 Certificate Details



This Certificate Belongs To

Shows the certificate owner's X.500 distinguished name.

This Certificate Was Issued By

Shows the issuer of the Certificate (the Certificate Authority). In addition to the main attributes, this field also shows the issuer's Certificate's serial number.

Validity Dates

The starting and ending Dates through which the certificate is valid (for example, 01/29/98 to 01/29/99).

Certificate Fingerprint

The unique identifier that is derived from MD5 hashing the certificates. The identifier should be compared with the fingerprint supplied directly from the certificate's issuer (for example, a CA). If the fingerprints do not match exactly, the certificate has been forged or modified.

Default Group

Drop-down list of the existing default groups.

Association of Certificate Subject DN with groups

For each trusted CA, shows a set of associations between certificates' subject DNs and group profiles. You can edit or delete existing associations by clicking on the appropriate buttons. You can also click on the Add button to add an association between the subject DN and a group profile.

Certificate Revocation List

Enabled

Click to enable the Certificate Revocation List (CRL) feature.

CRL usage is enabled on the switch on a per CA basis. To enable the use of CRLs for a CA, select the Details button on the main System→Certificates screen. The section labeled Certificate Revocation List Information is used to configure the necessary information. The Enabled check box turns on CRL checking of certificates for the particular CA. The Search Base, Host, Connection, and Update frequency values must be set for proper access to the CRL LDAP directory store.

Search Base

The search base represents the portion of the X.500 directory where the CA stores certificate revocation lists. Following is a sample search base entry:

```
ou=Engineering, o=Nortel Networks, c=US
```

Host

This field contains the host name or IP address of the LDAP-accessible directory server that is storing the published CRLs. This host must be reachable via one of the switch's private interfaces, and if a host name is used in place of an IP address, then one or more DNS servers must be configured on the switch's System→Identity screen.

Connection

Enter the port number that is associated with the LDAP server. Optionally, enable the use of the Secure Socket Layer (SSL) to secure the connection with the LDAP server. SSL is not required in general for handling CRLs since a CRL is signed and is therefore protected against modification and spoofing.

Status

The status field is read-only and is automatically updated by the switch to reflect CRL updating activity.

Update Frequency

Enter a value in minutes that represents the frequency with which the switch should query the CA's LDAP server for a newly published CRL. The default value 0 indicates that this switch does not update any CRLs. This is useful when many switches share an LDAP database, but you want only one switch to actually perform the update operation. To minimize the load on an external LDAP server, it is important to make sure only 1 or 2 switches are updating a shared CLR entry in a multiple switch, shared external LDAP environment.

Switch Settings

The System→Settings screen lets you configure Safe Boot mode and the serial port.

Figure 26 System→Switch Settings

Switch Settings

Safe Mode Configuration

Enable Safe Mode ☐

Safe Mode Duration 5 minutes (before reboot in normal mode attempted)

Note: Changes to Enable Safe Mode only take effect after a proper shutdown. Changes to Safe Mode Duration only take effect after the next Safe Mode Configuration create on the Admin→Config page.

Serial Port Configuration

Menu Access Level Unrestricted

Mode Serial Menu

Baud Rate 9600

Modem Initialization ATZ

Reset Serial Port Reset

Log File Configuration

Log File Life Time 60 Days

OK Cancel

NORTEL NETWORKS

Safe Mode Configuration

The switch can be booted in one of the two system modes: Safe Mode or Normal Mode. Each mode has its own software image, configuration files, and LDAP database.

A system booted in Safe Mode is only allowed to accept secured management tunnel establishment. When the secured management tunnel is established, Telnet, HTTP, and FTP traffic are allowed to come into the switch; no other VPN traffic is allowed through the secured management tunnel or the switch.

In Normal Mode, the system operates with the normal software and configuration and transports both VPN traffic and management traffic.

Enable Safe Mode

Use this check box to enable and disable Safe Mode.

Safe Mode Duration

The Safe Mode Duration setting determines how long the system operates in Safe Mode before attempting to reboot in Normal Mode.

Serial Port Configuration

The Serial Port Configuration section of the System-Settings screen provides options for configuring the switch's serial port. The parameters that you must set to enable your switch to communicate via the serial port are described below.

Whenever you change from either serial menu mode to PPP mode, or vice versa, you must restart the switch for the change to take effect.

Menu Access Level

The Menu Access Level setting determines which commands are available in a serial console port menu.

- Unrestricted - All commands are available to the user (default).
- Restricted 1 - System Reset commands plus the commands to change interface IP address and mask.
- Restricted 2 - Only Reset commands are available.

Mode

Select one of the following Modes of operation:

- Serial Menu (default)
- PPP
- Auto Detect

Serial Menu

In this mode, a standard menu interface is presented. You can use an application such as Hyper Terminal, when directly connected to the switch, to access the menu interface. The switch uses the COM port for a serial menu terminal session. The switch's serial port baud rate is 9600 by default. When you change the serial interface baud rate, you must press the Reset button.

PPP

You can set up the switch to use the Point-to-Point Protocol (PPP) over the serial port. This feature allows you to manage the switch from a remote location using PPP and the serial interface. If the switch were to become unreachable over the Internet, you could still dial up and manage it through the serial interface menu.

This feature allows you to access all of the management services (HTTP, Telnet, FTP, SNMP) through the Web interface. When a session is established through PPP, the serial interface acts as a private WAN interface with an internal IP address (0.0.1.35).

Auto Detect

This feature automatically detects whether the switch is using PPP or serial menu mode at startup. It cannot determine the switch's baud rate, nor can it determine a change from PPP to serial menu mode, except upon startup.

Auto Detect checks the mode each time the switch is restarted. When performing its Auto Detect check, the switch sends out AT command set characters to configure a modem if one is attached.

When the switch is in Auto Detect mode, and if a terminal session is connected and the terminal baud rate is the same as the switch's, the terminal displays the AT command sets on the screen. Simply press Enter more than five times before a serial menu session is started.

Baud Rate

Select one of the following Baud Rates to match the baud rate of your terminal:

- 57600
- 38400
- 19200
- 9600 (default)

Modem Initialization

Enter the modem initialization string. Refer to the manufacturer's documentation to learn the vendor-specific character initialization string. Preconfiguring the modem and using the switch's default initialization string (ATZ) provide the best results.

A sample 3Com/US Robotics 56K modem initialization string to instruct the external modem to connect at 19,200 Kbps follows:

```
ATZ&B1AT&N10
```

Reset Serial Port

When you select the baud rate, you must click the Reset button to change the port to the new baud rate.

Log File Configuration

The Log File Configuration sets the life time of the log files. The default log file life time is 60 days. You can set the file life time to any of the .

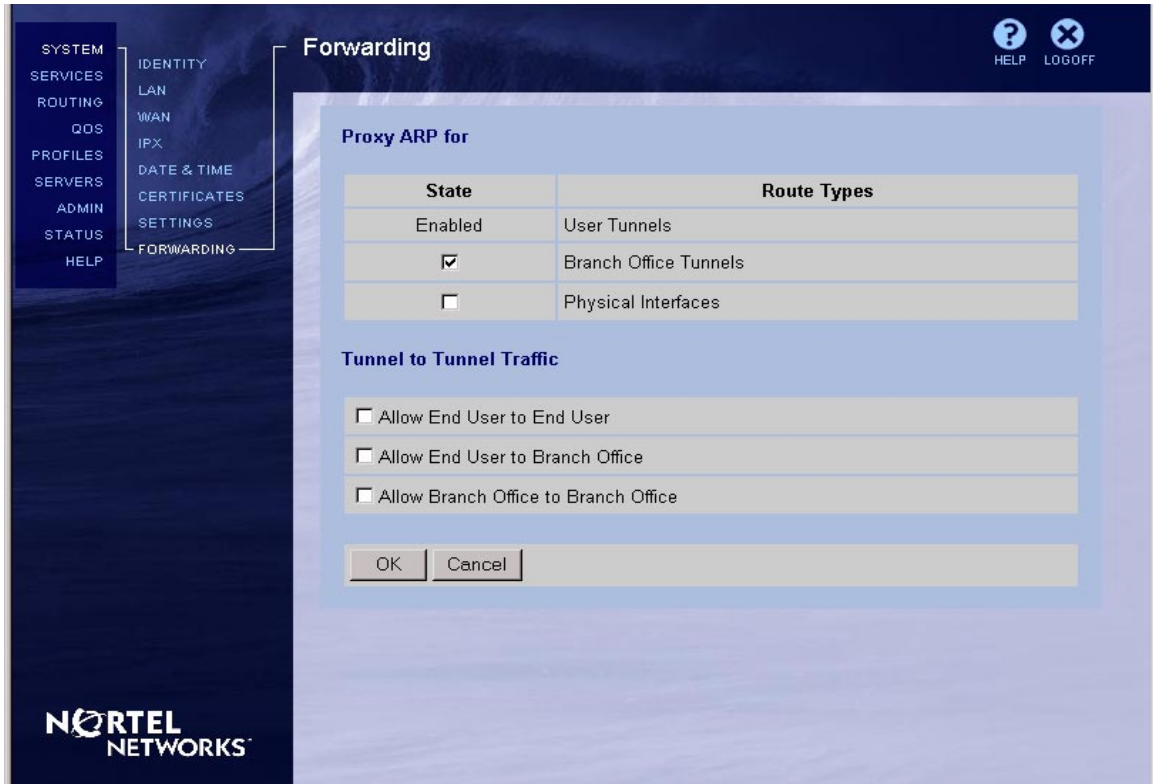
Log File Life Time

Select a value for the log file life time.

Forwarding

The System→Forwarding page allows you to configure Proxy ARP settings and Tunnel to Tunnel traffic settings.

Figure 27 System Forwarding



Proxy ARP for

The Contivity VPN Switch can be configured to respond to ARP requests on any of the physical interfaces. The switch responds to the following types of routes:

- User Tunnels are routes created for user tunnels. This entry is enabled by default and cannot be changed.
- Branch Office Tunnels are routes available through branch office connections. This option is disabled by default.

- Physical Interfaces are routes available through physical interfaces. This option is disabled by default.

Tunnel to Tunnel Traffic

Click the appropriate check boxes to enable the different types of tunnel-to-tunnel traffic. All of these options are **disabled** by default for security reasons.

Allow End User to End User

Click to allow a remote user who is tunneled into the corporate switch to access other remote users that are also tunneled into the switch.

Allow End User to Branch Office

Click to allow a remote user who is tunneled into the corporate switch to access the resources of branch offices that are connected to the switch.

Allow Branch Office to Branch Office

Click to allow users who are on one branch office connected to your switch to access resources on other branch offices that are connected to your switch.

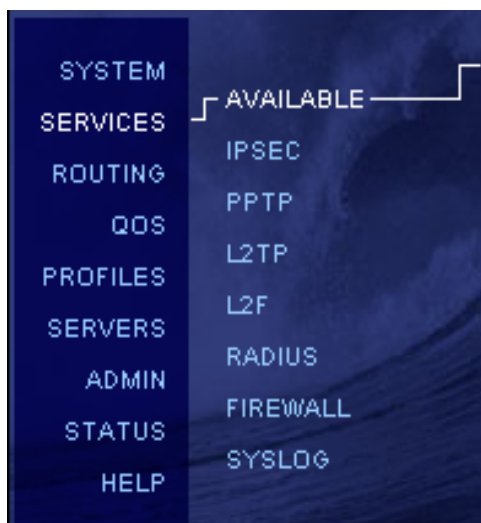
Chapter 2

Services

When you click on the Services menu, the list of services appears in the top left column.

The Services screen allows you to manage the available services, control the type of tunnel access to the Switch, and configure how the RADIUS service and the Firewall service are used. You can also specify the management and service protocols that can be used by the Switch.

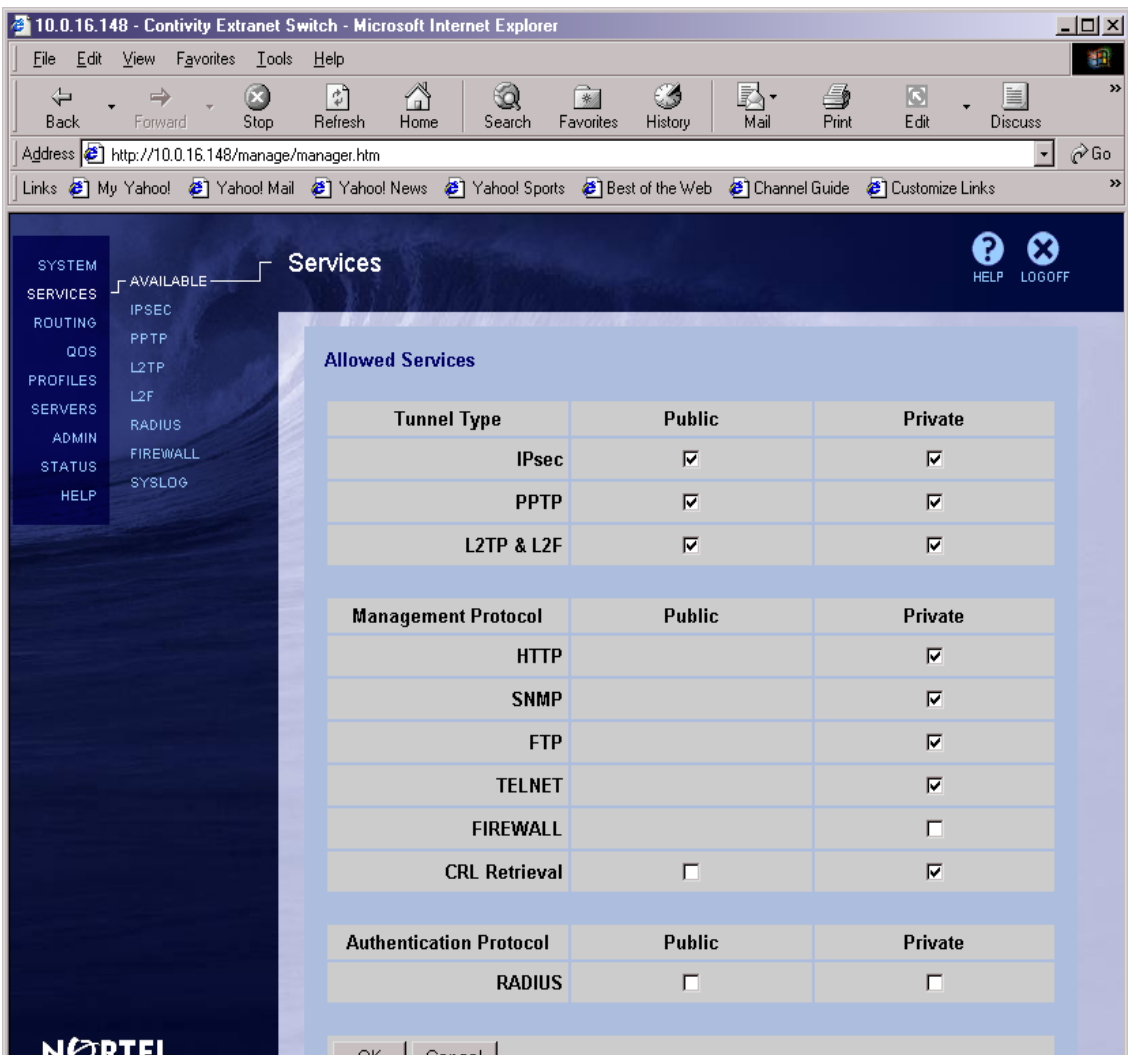
Figure 28 Services menu



Available Services

The Available Services include Tunnel Types, Management Protocols, and Authentication Protocol.

Figure 29 Available Services



Allowed Services

The Allowed Services include Tunnel Types, Management Protocols, and Authentication Protocol.

Tunnel Types

The Tunnel Type portion of this screen allows you to control each of the supported tunneling protocols on Private and Public interfaces. All tunneling protocols are enabled on the Public and Private networks by default. Since data in tunnels is encrypted, this default setting guarantees that all interactions with the Switch are private. To prevent tunnel connections of a particular type (for all users including Administrators), you can simply disable the tunnel type here.

For example, if you want to use IPSec as your only Public tunneling protocol, then disable the Public selection (remove the checkmark) for PPTP, L2TP, and L2F. By leaving IPSec, PPTP, L2TP, and L2F enabled on the Private side, you can establish tunneled connections to the Switch using any of the tunnel types from within your corporation (Private).

Management Protocols

Management related protocols are used on the Switch's Private Interfaces. Use the Available Services screen to control which management protocols can be accessed directly from a private LAN. Enabling Management Protocols allows you to access the Switch for management purposes in a nontunneled environment, if the filter permits (refer to "Edit Filter").

As network administrator, you might decide to deny access to the HTTP or SNMP protocols coming through private nontunneled connections. This ensures that Switch management can be accomplished through tunneling only.



Caution: Make sure that the tunneling features are working properly before you disable the local HTTP management option. Otherwise, you cannot manage the Switch.

Similarly, you might want to prohibit the ability to transfer files to or from the system using FTP for security reasons.



Note: After your initial system configuration, you might want to disable Private HTTP access and restrict access to Tunneled connections only.

Table 5 Management Protocols

Management Protocol	Description
HTTP	HyperText Transfer Protocol is the software protocol that allows Web servers and clients to communicate (it allows for an HTML management interface).
SNMP	Simple Network Management Protocol is the Internet standard that allows you to manage devices and receive traps on an IP network. Due to security reasons, the Switch supports SNMP MIB II get commands only.
FTP	File Transfer Protocol is a TCP/IP protocol that allows you to transfer files between systems over a network.
Telnet	Telnet is the virtual terminal protocol that allows users on one device to access and manage a remote device. Telnet is used by Nortel Networks Customer Support personnel strictly for maintenance purposes. Telnet has direct access to the Switch System Services and therefore should normally be disabled for security reasons. Telnet must be enabled in order to use the CLI via Telnet.
FIREWALL	The FireWall-1 management protocol that is used for communication between the FireWall-1 Management Station and the integrated CheckPoint FireWall-1 running on the Switch.
CRL Retrieval	Enables retrieval of CRLs through the selected interface type. Both interfaces can be enabled at the same time. Refer to "SSL and Digital Certificates" for information about Digital Certificates.

Authentication Protocols

RADIUS

Use the RADIUS check boxes to permit RADIUS requests on the public and private interfaces of the Switch. If you enable RADIUS traffic on this screen, the settings on the Services→RADIUS screen are used (RADIUS must also be enabled on that screen).

IPSec Settings

The IP Security (IPSec) standard defines a set of security protocols that:

- Authenticate IP connections.
- Add data confidentiality and integrity to IP packets.
- Are transparent to applications and the underlying network infrastructure.

IPSec supports multiple encryption and authentication protocols so that your security policy can dictate levels of data privacy and authentication. IPSec also supports load balancing and fail-over.

IPSec allows for multivendor interoperability. It uses a flexible key management scheme called the Internet Security Association Key Management Protocol (ISAKMP), which enables peer connections to quickly and dynamically agree on compatible security and connection parameters (keys, encryption, and authentication).



Note: To allow RADIUS authentication with the IPSec client you must enable the RADIUS server on the Profiles→Groups→Edit→IPSec screen.

Figure 30 IPSec Server

Authentication

User Name and Password/Pre-Shared Key	☒
RSA Digital Signature	☒

RADIUS Authentication

AXENT Technologies Defender	☒
Security Dynamics SecurID	☒
User Name and Password	☒

Encryption

ESP - 56-bit DES with SHA1 Integrity	☐
ESP - 56-bit DES with MD5 Integrity	☒
ESP - 40-bit DES with SHA1 Integrity	☐
ESP - 40-bit DES with MD5 Integrity	☒
ESP - NULL (Authentication Only) with SHA1 Integrity	☐
ESP - NULL (Authentication Only) with MD5 Integrity	☐
AH - Authentication Only (HMAC-SHA1)	☒
AH - Authentication Only (HMAC-MD5)	☒

Authentication Order

Order	Server	Type	Associated Group	Action
1	LDAP	Internal		
2	RADIUS	CHAP, PAP	/Base	Delete

Load Balance

Load Balance	Enabled	Management IP Address
Alternate Host	☐	

Fail-Over

Fail-Over	Enabled	Public IP Address
Host 1	☐	
Host 2	☐	
Host 3	☐	

Authentication

User Name and Password/Pre-Shared Key

Click to enable authentication with a username and password.

RSA Digital Signature

Click to enable authentication with an RSA Digital Signature.

RADIUS Authentication

Click to Enable support for the authentication types that your RADIUS Server supports and that you expect to use:

- AXENT Technologies Defender--AXENT OmniGuard/Defender authentication.
- Security Dynamics SecurID--Security Dynamics SecurID authentication.
- User Name and Password--Username and password authentication; the username and password are encrypted.

Encryption

Click the appropriate checkbox to either enable or disable the supported Encryption methods for this group.



Note: Using higher-level encryption, such as Triple DES, decreases performance.

The encryption methods are shown on the screen in order of strength, from strongest to weakest. All of the encryption methods ensure that the packet came from the original source at the secure end of the tunnel. Some of the encryption types do not appear on non-US models that are restricted by US Domestic export laws.

If two devices have different encryption settings (due to either US export laws or administrative configuration), the two devices negotiate downward until they agree on a compatible encryption capability. For example, if a Switch in the US attempts to negotiate Triple DES encryption with a Switch in Australia that is using 56-bit DES, then the Australian Switch rejects Triple DES encryption in favor of the 56-bit DES.

The following table shows a comparison of the security provided by the available encryption and authentication methods.

Table 6 Comparing Encryption and Authentication Methods

Method		Encryption of IP Packet Payload	Authentication of IP Packet Payload	Authentication of Entire IP Packet
ESP	Triple DES SHA1	Yes	Yes	No
	Triple DES MD5	Yes	Yes	No
	56-bit DES SHA1	Yes	Yes	No
	56-bit DES MD5	Yes	Yes	No
	40-bit DES SHA1	Yes	Yes	No
	40-bit DES MD5	Yes	Yes	No
	NULL SHA1	No	Yes	No
	NULL MD5	No	Yes	No
AH	HMAC SHA1	No	No	Yes
	HMAC MD5	No	No	Yes

The following topics describe important aspects and terminology to aid you in selecting the appropriate encryption method for your tunnel server.

Types of Integrity Checks

The Switch uses the following two types of integrity checks:

- **SHA1**

The Secure Hash Algorithm (SHA1) produces a 160-bit hash. It is regarded by cryptographers as being more resistant to attacks than MD5. It does not encrypt data.

- **MD5**

The Message Digest 5 Algorithm (MD5) is used to confirm the authenticity of a packet. It produces a 128-bit hash. It does not encrypt data. Also, MD5 provides integrity that detects packet modifications.

- **HMAC**

The Hashed Message Authentication Code (HMAC) is a technique that uses a secret key and a message digest function to create a secret message authentication code. The HMAC method strengthens the SHA1 and MD5 technique.

Encapsulating Security Payload (ESP)

The Encapsulating Security Payload (ESP) provides confidentiality for IP datagrams by encrypting the payload data to be protected. Data Encryption Standard (DES) is an encryption block cipher algorithm. The Switch supports the following variants of the DES algorithm:

- Triple DES uses a 168-bit key. It uses the DES encryption algorithm three times. The first 56 bits of the key is used to encrypt the data, then the second 56 bits is used to decrypt the data. Finally, the data is encrypted once again with the third 56 bits, which triples the algorithm's complexity.
- 56-bit DES and 40-bit DES use their respective 56-bit or 40-bit key (with 8 bits of parity) over a 64-bit block. The 56 or 40 bits of the key are transformed and combined with a 64-bit message through a complex process of 16 steps.
- Both 56- and 40-bit DES require the same processing demands, so you should use 56-bit DES unless local encryption laws prohibit doing so.
- The Null specification provides authentication only. No encryption is done.

Authentication Header (AH)

Authentication Header (AH) provides data integrity and source authentication. The AH method does *not* encrypt data.

The use of a NAT device in the tunnel path can sometimes cause the AH method to report a security violation.

IKE Encryption and Diffie-Helman Group

On this screen, you set the global IKE encryption and Diffie-Helman group for IPSec. If you select, the Both 56-bit DES with Group 1 and Triple DES with Group 2 option, you can edit this field on the Profiles→Branch Office→Edit→IPSec screen or the Profiles→Groups→Edit→IPSec screen.

From the drop-down list, select one of the following:

- Both 56-bit DES with Group 1 and Triple DES with Group 2
- Triple DES with Group 2 (1024-bit prime)
- 56-bit DES with Group 1 (768-bit prime)

Authentication Order

The IPSec, PPTP, L2TP, and L2F tunnel types each have an Authentication Order table, which lists the corresponding servers, authentication types, associated groups, and actions. The LDAP server is always queried first, then RADIUS, if applicable. The Authentication Order descriptions that follow are the same for each tunnel type.

Order

Shows the order of authentication preference.

Server

The Switch supports LDAP and RADIUS authentication servers. The Switch always attempts to authenticate a remote user against the LDAP database. If a User ID (UID) and password are found, the Switch uses the attributes that are defined for that user's group.

The Switch can also authenticate against a RADIUS database. When using RADIUS for authentication, you can assign LDAP groups to users in the RADIUS database to take advantage of different profiles, or you can simply assign all RADIUS users into a single "default" group. The default RADIUS group is stored in the LDAP database. Refer to "RADIUS Authentication Class Attribute Values" for additional information on RADIUS Authentication Class Attributes and their relationship to an LDAP database.

Type

LDAP can be either an Internal or External server.

The types of RADIUS authentication currently associated with the server are:

- AXENT--This is AXENT OmniGuard/Defender challenge response token security authentication. The AXENT OmniGuard/Defender uses a personal identification number (PIN) and password, coupled with a challenge response security dialog box, to authenticate user identity.
- SecurID--This is Security Dynamics SecurID token security authentication. The SecurID uses a PIN and the current code generated by a token assigned to the user to authenticate user identity.
- CHAP--This is the Challenge Handshake Authentication Protocol (CHAP).
- MS-CHAP--This is a Microsoft variant of CHAP that includes data encryption.
- PAP--This is Password Authentication Protocol.

Associated Group

This is the Group from which authorization and operational settings are taken if a group attribute is not found in the authentication database.

Action

Delete--Click to remove the configured server. You are prompted to confirm your deletion request.

Add--Click to add an authentication type.

Load Balance

Click to enable Load Balancing of one Switch with an alternate Switch. Load Balancing is a protocol between two Switches that exchanges information about the number of sessions of each connection priority and the CPU utilization. When a connection is being established, the first Switch determines which of the two Switches should service the session. The Switch and the alternate Switch must be in the same location (they must be in communication via the private interface).

Management IP Address

Enter the private management IP address of the Switch that you want to serve as the alternate Switch for Load Balancing.

Fail-Over

Click to enable Fail-over of the selected Switch. A Fail-over condition is detected in approximately two minutes. If a connection is somehow terminated or lost, the client then attempts to connect to the first-listed Fail-over Switch. It tries each Switch in succession and if no connection is established, it stops.

The Switch IP addresses (do not use domain names) must be public interfaces if the Switches are in remote locations. Also, alternate Switches should mirror the same configuration as the primary Switch; otherwise, the connection information on the client does not match and results in authentication failures.

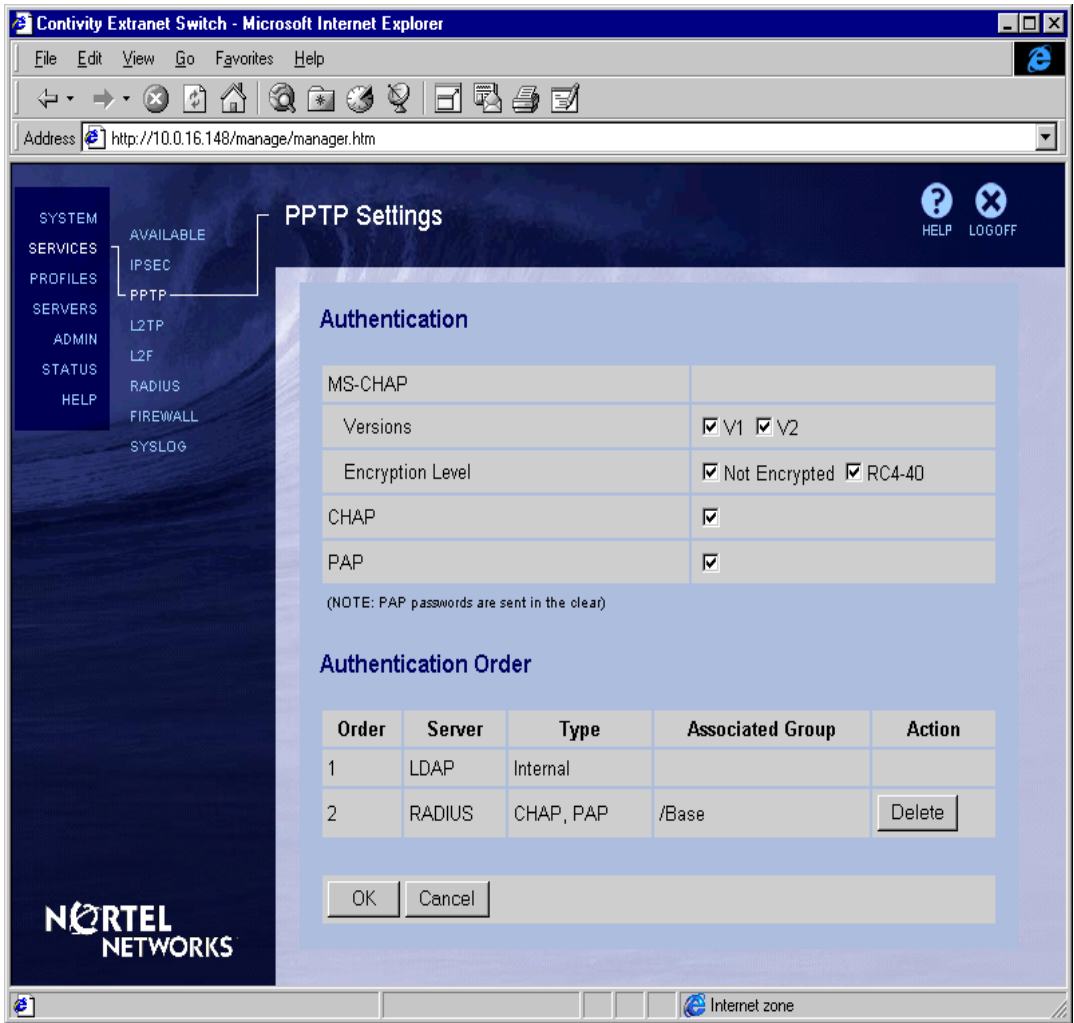
Public IP Address

Enter the public IP address of the Switches to which you want to Fail-over in case the primary Switch connection terminates.

PPTP Settings

The Point-to-Point Tunneling Protocol (PPTP) is supported by Nortel Networks, Microsoft, and other vendors. The PPTP client is available for Windows 95 and is built-in to Windows 98 and Windows NT®. Third-party vendors have developed PPTP clients for Windows 3.1 and the Macintosh operating system.

Figure 31 PPTP Server



Authentication

PPTP settings allow you to select a specific authentication server type; for example, RADIUS. Each server type allows you to specify an authentication scheme: MS-CHAP, CHAP, or PAP.



Note: Not all RADIUS servers support all forms of authentication. Failure to match PPP authentication methods with RADIUS server capabilities results in user-authentication failures. Check your vendor's RADIUS documentation for additional information.

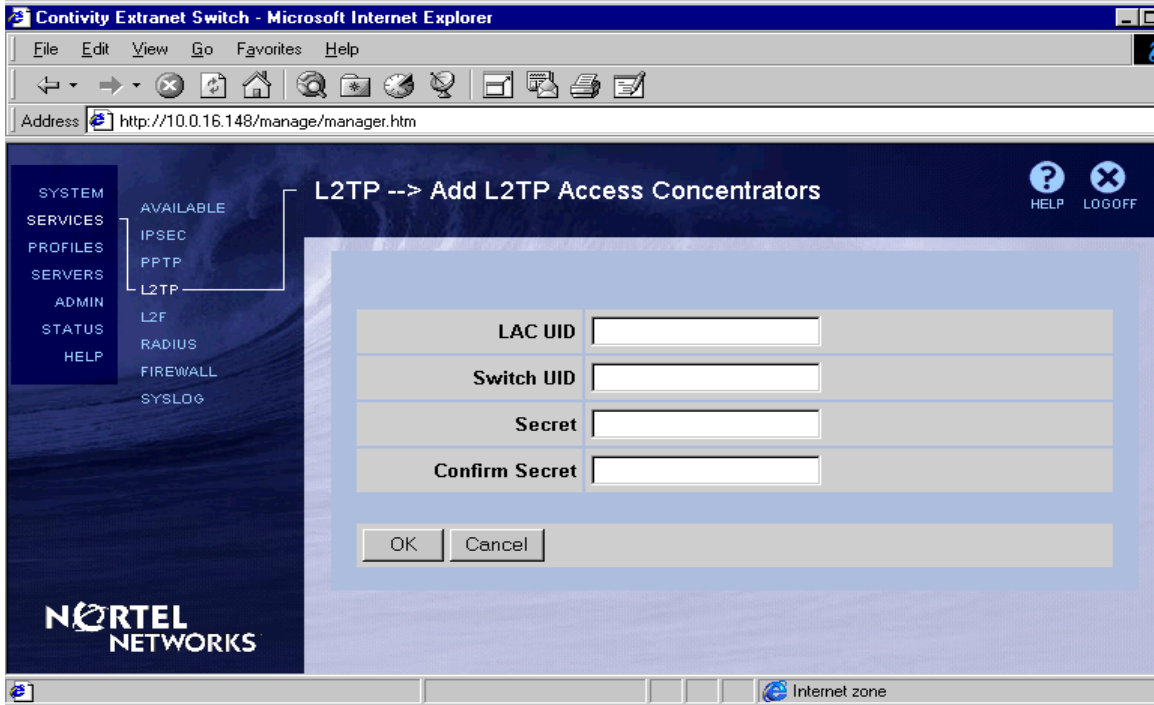
Authentication Order

The Authentication Order table lists the corresponding servers, authentication types, associated groups, and actions. The LDAP server is always queried first, then RADIUS, if applicable. Refer to “Authentication Order” for a description of the Authentication Order table.

L2TP Settings

The Layer 2 Tunneling Protocol (L2TP) is supported by Nortel Networks, Cisco Systems, Microsoft, and other vendors.

Figure 32 L2TP Server



Authentication

L2TP settings allow you to select a specific authentication server type; for example, RADIUS. Each server type allows you to specify an authentication scheme: MS-CHAP, CHAP, or PAP.



Note: Not all RADIUS servers support all forms of authentication. Failure to match PPP authentication methods with RADIUS server capabilities results in user-authentication failures. Check your vendor's RADIUS documentation for additional information.

Authentication Order

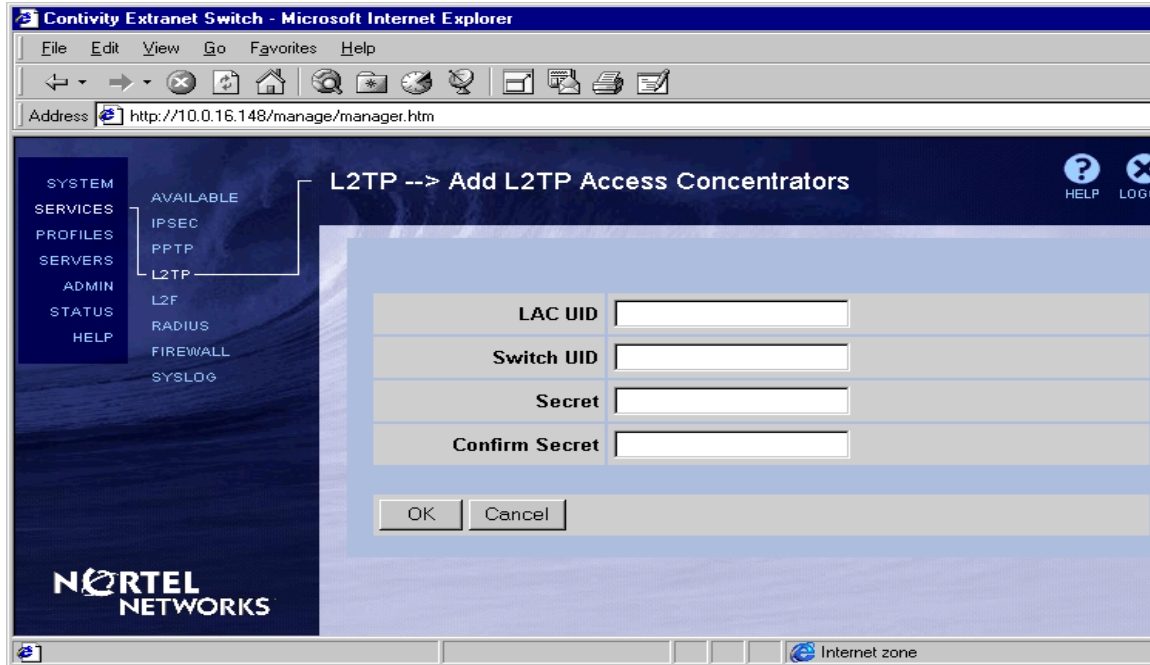
The Authentication Order table lists the corresponding servers, authentication types, associated groups, and actions. The LDAP server is always queried first, then RADIUS, if applicable. Refer to “Authentication Order” for a description of the Authentication Order table.

L2TP Access Concentrators

- Delete—Click to remove the configured concentrator. You are prompted to confirm your deletion request.
- Add—Click to go to the Add L2TP Access Concentrator.
- Edit—Click to go to the Edit L2TP Access Concentrator screen and modify the settings of an existing concentrator.

L2TP Add or Edit Access Concentrators

The L2TP Add Access Concentrators screen allows you to configure the authentication between the Switch and the NAS. Use the Edit Access Concentrators screen to modify the information for an existing concentrator.

Figure 33 L2TP Add or Edit

LAC/Switch

LAC/Switch UUIDs

Enter the agreed upon User IDs (UUIDs) for the LAC (L2TP Access Concentrator) and the Switch. UUIDs must be coordinated between you and the NAS provider.

Secret

Enter the agreed upon Secret (password) for the LAC (L2TP Access Concentrator) and the Switch. Secrets must be coordinated between you and the LAC provider.

Confirm Secrets

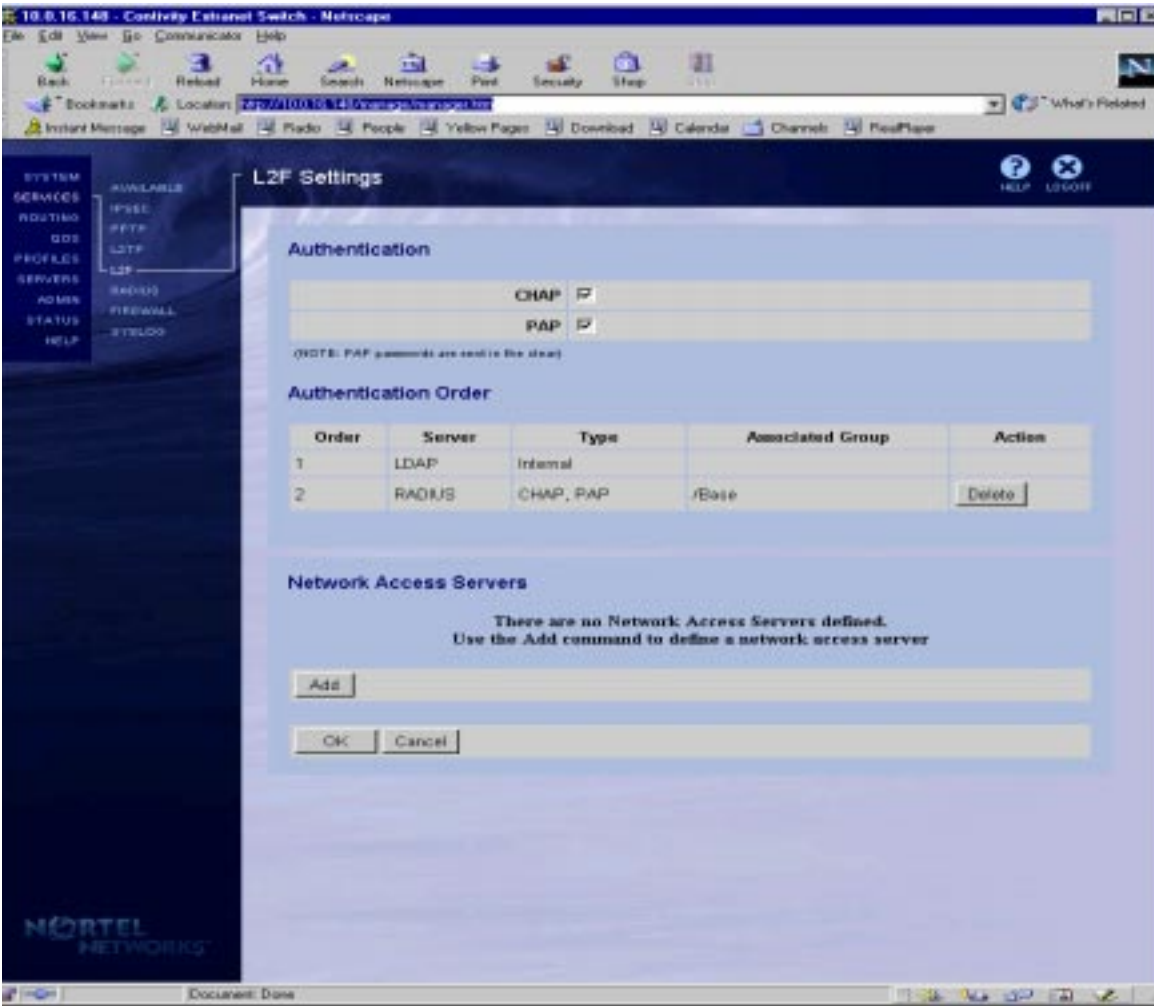
Reenter the assigned Secret (password) to verify that you have typed the intended Secret correctly.

L2F Settings

The L2F (Layer 2 Forwarding) is a tunneling protocol supported by Nortel Networks, Cisco Systems, Shiva, and other vendors. L2F tunneling provides remote access to corporate networks across the public Internet. L2F tunnels are generally established between the network access server (NAS) at the Internet service provider (ISP) and the Switch.

In addition to user authentication, L2F requires you to provide NAS and Switch user IDs and passwords.

Figure 34 L2F Settings



Authentication

L2F allows you to add a RADIUS server for authentication. The Authentication portion of this screen allows you to specify an authentication scheme or either CHAP or PAP.

Authentication Order

The Authentication Order table lists the corresponding servers, authentication types, associated groups, and actions. The LDAP server is always queried first, then RADIUS, if applicable. Refer to “Authentication Order” for a description of the Authentication Order table.

Network Access Servers

This table provides the UUIDs for the network access servers (NAS) and Switch, and the possible Actions you can take. The NAS acts like a middleman between the remote user and the Switch. It authenticates each side, and once validation is complete, a tunnel is formed. The user has a standard connection (for example, PPP) to the NAS, but an L2F tunnel is formed between the NAS and the Switch.

NAS/Switch UUIDs

Names/Passwords

UUIDs allow the NAS and the Switch to mutually authenticate each other. The NAS UUID is used by the NAS to log into the Switch, and the Switch ID is used by the Switch to log into the NAS.

Action

Delete—Click to remove an existing NAS entry. You are prompted to confirm your deletion request.

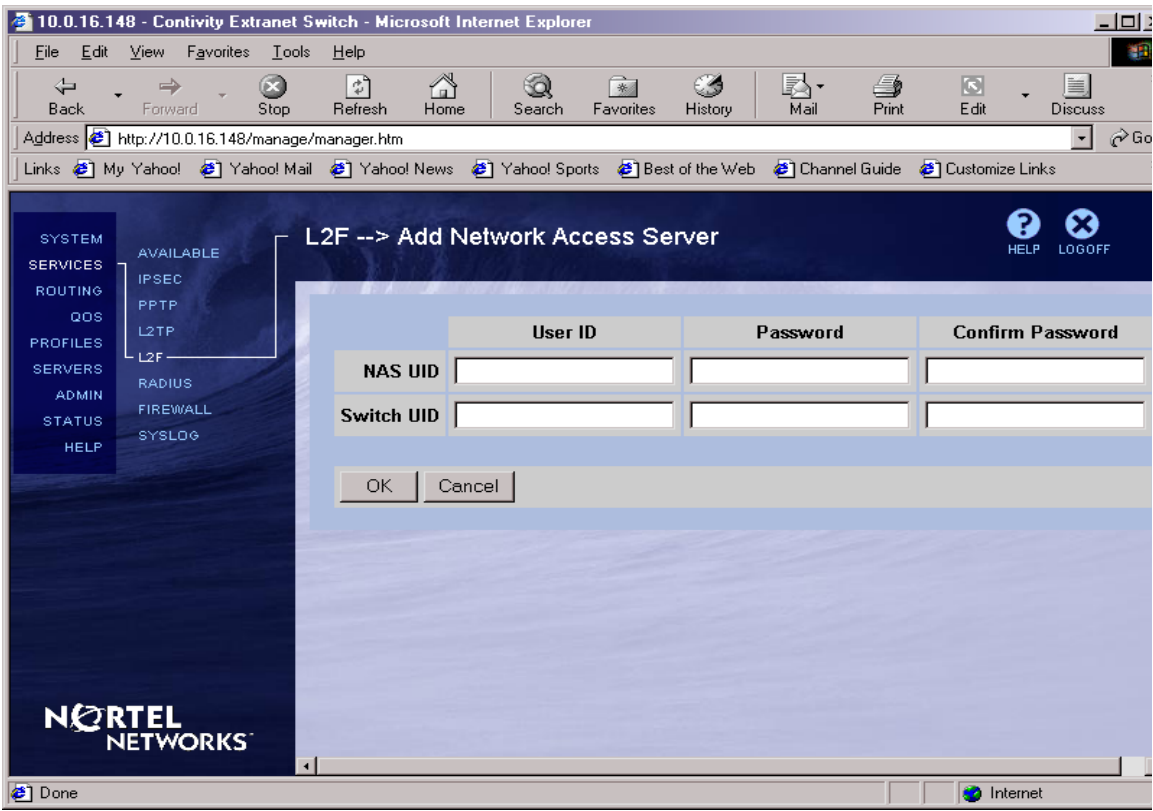
Add—Click to go to the Add Network Access Server screen.

Edit—Click to go to the Edit L2TP Access Concentrator screen and modify the settings of an existing NAS.

L2F Add or Edit Network Access Server

The L2F Add Network Access Server screen allows you to configure the authentication between the Switch and the network access server (NAS). Use the L2F Edit Network Access Server screen to modify the information for an existing server.

Figure 35 L2F Add Network Access Server



NAS/Switch

NAS/Switch UIDs

Enter the agreed upon user IDs (UIDs) for the NAS and the Switch. UIDs must be coordinated between you and the NAS provider.

Passwords

Enter the agreed upon Passwords for the NAS and the Switch. Passwords must be coordinated between you and the NAS provider.

Confirm Passwords

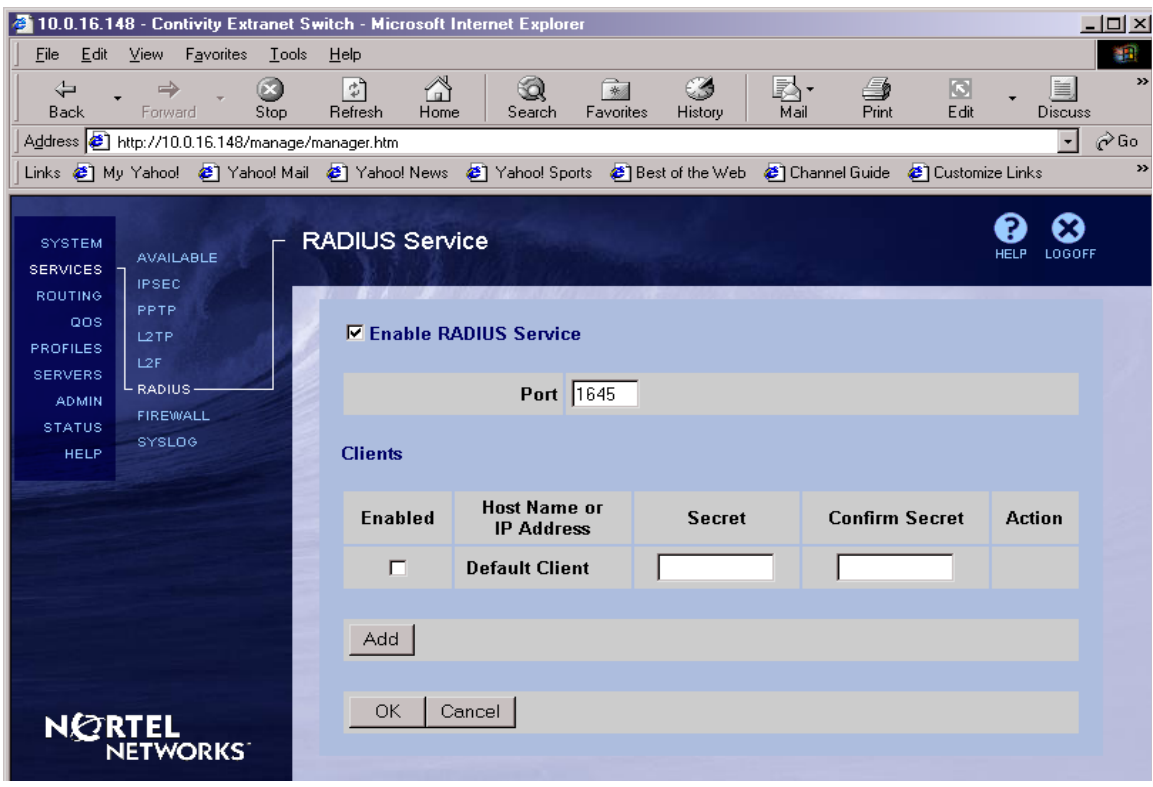
Reenter the assigned password to verify that you have typed the intended password correctly.

RADIUS Service

The RADIUS Service feature allows the switch to function as a simple RADIUS server.

For users with multiple user accounts, RADIUS Service attempts to authenticate against each account type. If the given username/password matches any of the user's accounts, the authentication succeeds. The authentication is done in this order: PPTP, IPsec, L2F, L2TP.

Figure 36 RADIUS Service



Enable RADIUS Service

Click to enable RADIUS Service. The Switch now listens on the specified port for authentication requests from remote RADIUS clients.

 **Note:** You must also have RADIUS enabled as an available service on the Services→Available screen. Refer to “Authentication Protocol” for details.

Port

Enter the Port number on which the Switch listens for authentication requests from remote RADIUS clients. Port 1645 is the default port number, which is commonly used. However, port 1812 is the port number specified by the RADIUS RFC.

Clients

The Clients section is used to specify the names of the remote hosts that are permitted to send or forward authentication requests to your Switch.



Note: Do not confuse the use of the term “Clients” on this screen with a remote Contivity VPN Client, such as an IPSec tunnel client. Clients on this screen denotes a RADIUS client. These clients are network access devices or RADIUS servers (usually belonging to an ISP), that can initiate or forward (proxy) authentication requests to the Switch.

Enabled

Click to allow the Switch to receive authentication requests from the specified RADIUS client.

Host Name or IP Address

The fully qualified domain name or IP address of the remote RADIUS client from which the Switch can receive authentication requests.

Default Client

The first entry in this column is the Default Client. The Default Client is a time-saving feature that enables a Switch administrator to allow all public authentication devices that know the specified secret to send or forward authentication requests to the Switch. Using this feature, the Switch administrator does not have to enter a Host Name or IP Address for each remote device that is a client for the RADIUS Service.

Switch administrators must weigh the convenience that the use of a Default Client provides against possible security implications.

You can disable the use of the default client, but you cannot delete the entry from the list. Initially, the Default Client is disabled (not checked).

Secret

The secret that authorizes the remote RADIUS client to connect to the Switch for authentication. You can change the secret on this screen.

Confirm Secret

If you change the secret, you must reenter it here to verify that you typed the new secret correctly.

Action

Delete

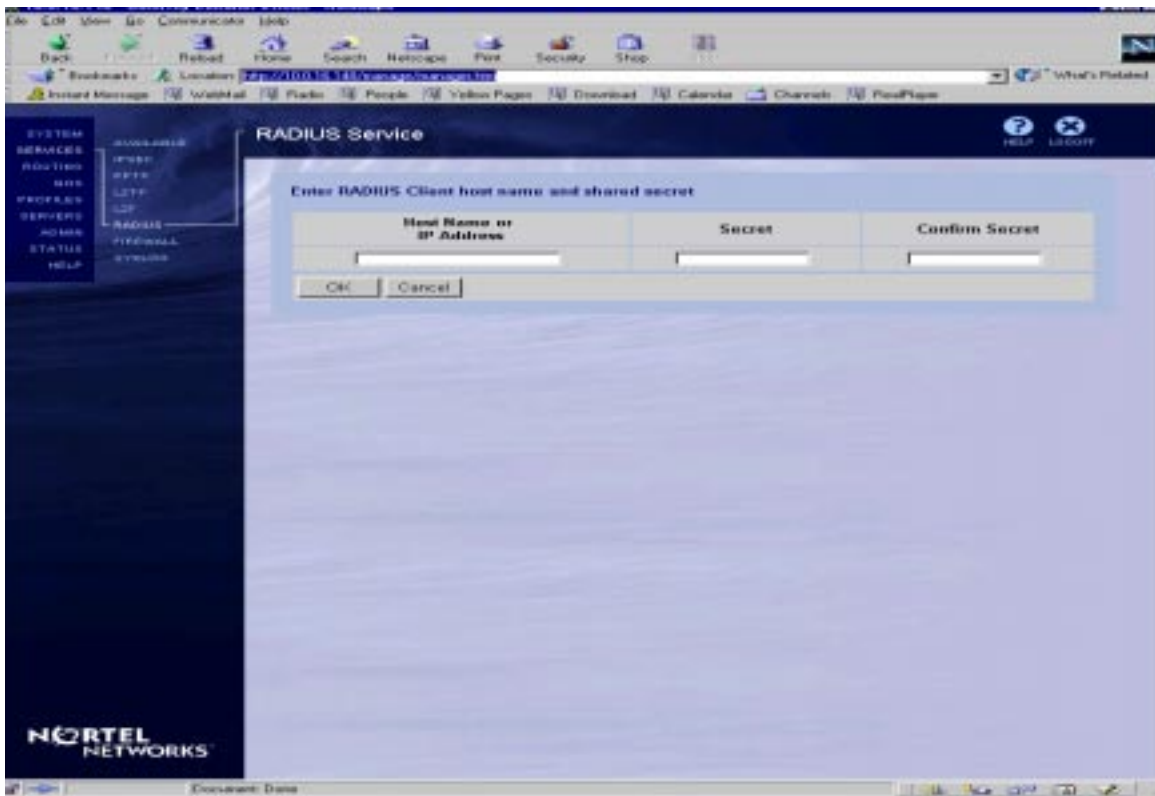
Click to remove the selected client. You are prompted to confirm your deletion request.

Add

Click to go to the Add RADIUS Service Client” screen.

Add RADIUS Service Client

The Add RADIUS Service Client screen appears when you click the Add button in the RADIUS Service screen.

Figure 37 Add RADIUS Service Client Screen

Host Name or IP Address

Enter either the fully qualified domain name or the IP address of the remote RADIUS Service client from which the Switch can receive authentication requests. The name is then listed on the RADIUS Service screen.

Secret

Enter the secret that authorizes the remote RADIUS Service client to connect to the Switch for authentication. You can later change the secret on the RADIUS Service screen.

Confirm Secret

Reenter the secret to verify that you typed it correctly.

Firewall/NAT

The Contivity provides a choice of three possible firewall solutions. With the addition of an integrated firewall, the switch can perform a variety of secure routing functions, depending upon how you set up the switch's routing capabilities. For example, you can configure the switch to securely route non-tunneled traffic from its private interface, through the firewall, and out its public interface. This configuration would enable users on the switch's private network to access the Internet without requiring a separate, dedicated router.

Figure 38 Services→Firewall/NAT screen

Firewall / NAT

Configuration

Enabled	Firewall / NAT Type	Firewall / NAT Policy	Action
☒	Contivity Firewall *		Edit
☐	Contivity Stateful Firewall	Policy: AllowAny	Manage Policies
☐	Contivity Interface Filter		
☐	Interface NAT	NAT Set: Overlap	NAT Configuration
☐	Anti-Spoofing		Edit
☐	Check Point FireWall-1		Edit
☐	No Firewall		

* To turn on Contivity Firewall, at least one of Contivity Stateful Firewall and Contivity Interface Filter should be enabled.

Contivity Tunnel Filter ☐ Enable

Note: Contivity Tunnel Filter can only be disabled when Contivity Stateful Firewall is enabled. It is typically enabled while you are migrating to the Stateful Firewall.

[OK](#) [Cancel](#) [Refresh](#)

Configuration

Enabled

Use this column to enable the Firewall/NAT Types you want to use.

By default the No Firewall option is selected.

Firewall/NAT Type

Contivity Firewall

Click to enable the Contivity Firewall. The Contivity Firewall must be enabled in order to run any combination of:

- Contivity Stateful Firewall
- Contivity Interface Filter
- Interface NAT
- Anti-Spoofing

Contivity Stateful Firewall

Check this box to enable the Contivity Stateful Firewall.

The Contivity Stateful Inspection Firewall allows you to statefully inspect traffic on all physical and virtual (tunnel) interfaces. Refer to "Managing the Contivity Stateful Firewall" for more information.

Contivity Interface Filter

Check this box to enable Contivity Interface Filter.

This option can be enabled at the same time as the Contivity Stateful Firewall, enabling you to migrate to the Contivity Stateful Firewall over time. It allows you to continue using existing interface filters with the Stateful Firewall while you build interface filters to regulate non-tunneled traffic and test the firewall policies live. This enables you to continue using the interface filters for traffic that you have not yet added interface rules for in the Stateful Firewall.

Once you are satisfied that the Stateful Firewall policy is correct (that is, it has all of the same rules as the old tunnel interface filters did) you can disable Contivity Interface Filters, and run *only* with the Contivity Stateful Firewall, which is much more efficient.

The policies in the Stateful Firewall take precedence over the interface filters.

Interface NAT

Check this box to enable Interface NAT. This option enables you to apply NAT rules to non-tunneled traffic that you route through the switch. Enabling and configuring Interface NAT here does not affect Branch Office NAT settings.

Anti-Spoofing

Check this box to enable Anti-Spoofing. Anti-spoofing prevents packets from passing into a private network with forged source addresses in the packet header. The source address of each packet entering the switch through a public interface and bound for a private interface is examined to ensure that the source address is not from a subnet reachable through a private interface or a tunnel.

You should disable Anti-Spoofing if you advertise direct routes (see Policy) over an interface and you have dynamic Branch Office tunnels defined over that interface, or the tunnel packets will get dropped due to Anti-Spoofing.

Check Point Firewall-1

Check this box to enable Check Point Firewall-1. See Check Point FireWall-1 Service.

No Firewall

Check this box to enable a No Firewall state.

Firewall/NAT Policy

Contivity Stateful Firewall Policy

This list-box shows the currently selected Contivity Stateful Firewall Policy being used and lists any additional ones from which you select.

Use the Manage Policies button to launch the CSF Manager applet to create and manage firewall policies. The new policies you create are not automatically applied to the firewall. You cannot apply a policy from the CSF Manager applet.

The system default policy means that the firewall is enabled and no policies are applied except for the implied rules.

NAT Set

This list-box shows the currently selected NAT set being used and lists any additional NAT sets.

You can use the NAT Configuration link to jump to the Profiles→NAT Sets screen to create a new NAT Set if you do not want to use any of the existing ones. You can then use the Return to Firewall/NAT Screen link to jump back to this screen and apply the new NAT Set.

Selection of a NAT set here applies to non-Tunneled traffic only. It does not affect the NAT sets applied to Branch Office tunnels. If any Branch Office tunnel NAT sets are assigned, they remain in effect for those Branch Office tunnels.

Actions

Edit Contivity Firewall

Click the Contivity Firewall Edit button to access the Edit screen for the Contivity Firewall. See *Edit Contivity Firewall*.

Manage Policies

Click the Manage Policies button to configure and manage the Contivity Stateful Firewall. This button launches the CSF Manager applet. Refer to *Managing the Contivity Stateful Firewall* for more information.

NAT Configuration

Click the NAT Configuration link to go to the Profiles→NAT Sets screen to configure NAT Sets. See *Network Address Translation (NAT)*.

Edit Anti-Spoofing

Click the Edit Anti-Spoofing button to configure Anti-Spoofing. See *Anti-Spoofing Configuration*.

Edit Check Point Firewall-1

Click the Edit button for the Check Point Firewall-1 to configure the Check Point Firewall-1. See Check Point FireWall-1 Service.

Anti-Spoofing Configuration

All public interfaces in the switch are listed on this page. You can configure Anti-Spoofing for each interface.

Anti-Spoofing Enabled

A check in this box indicates that Anti-Spoofing is enabled for the specific interface.

Public Interface

This field shows the name of the Interface.

IP Address

The IP Address of the Interface.

Edit Contivity Firewall

Click the Edit button for the Contivity Firewall on the Firewall/NAT screen to access the Contivity Firewall Edit screen. Use this screen to configure connection limits and logging activity for the Contivity Firewall.

Connection Number

Maximum Connection Number

Enter the maximum number of connections in this field. The connection number allows you to reserve memory for a maximum number of connections. The number range varies depending on the Contivity model and amount of memory on the Switch.

Determining the optimum memory allocation makes it easier to tune your system for firewall traffic. Because the Firewall tracks conversations, it pre-allocates memory.

Logging

Select the types of logging that you want in this section of the screen. These logging options apply only to information going into the EVENTLOG. None of the logged information gets sent to the SYSLOG.



Note: If any of these choices are selected and the switch is under a heavy load, the EVENTLOG could overflow, losing entries.

All

Check this box to enable logging of all activity.

Traffic

Check this box to log flow/conversation creation and deletion type messages to the EVENTLOG.

Policy Manager

Check this box to log policy/rule creation and processing type messages to the EVENTLOG.

Firewall

Check this box to log counts of packets dropped/allowed by Firewall processing to the EVENTLOG.

NAT

Check this box to log all Interface NAT related messages to the EVENTLOG. This does not cause logging of Branch Office NAT message.

Debug

Check this box to log additional debugging information. Because of the amount of logging this generates and the impact it could have on performance, you should enable this option only when advised to do so by a Nortel Networks Customer Support representative.

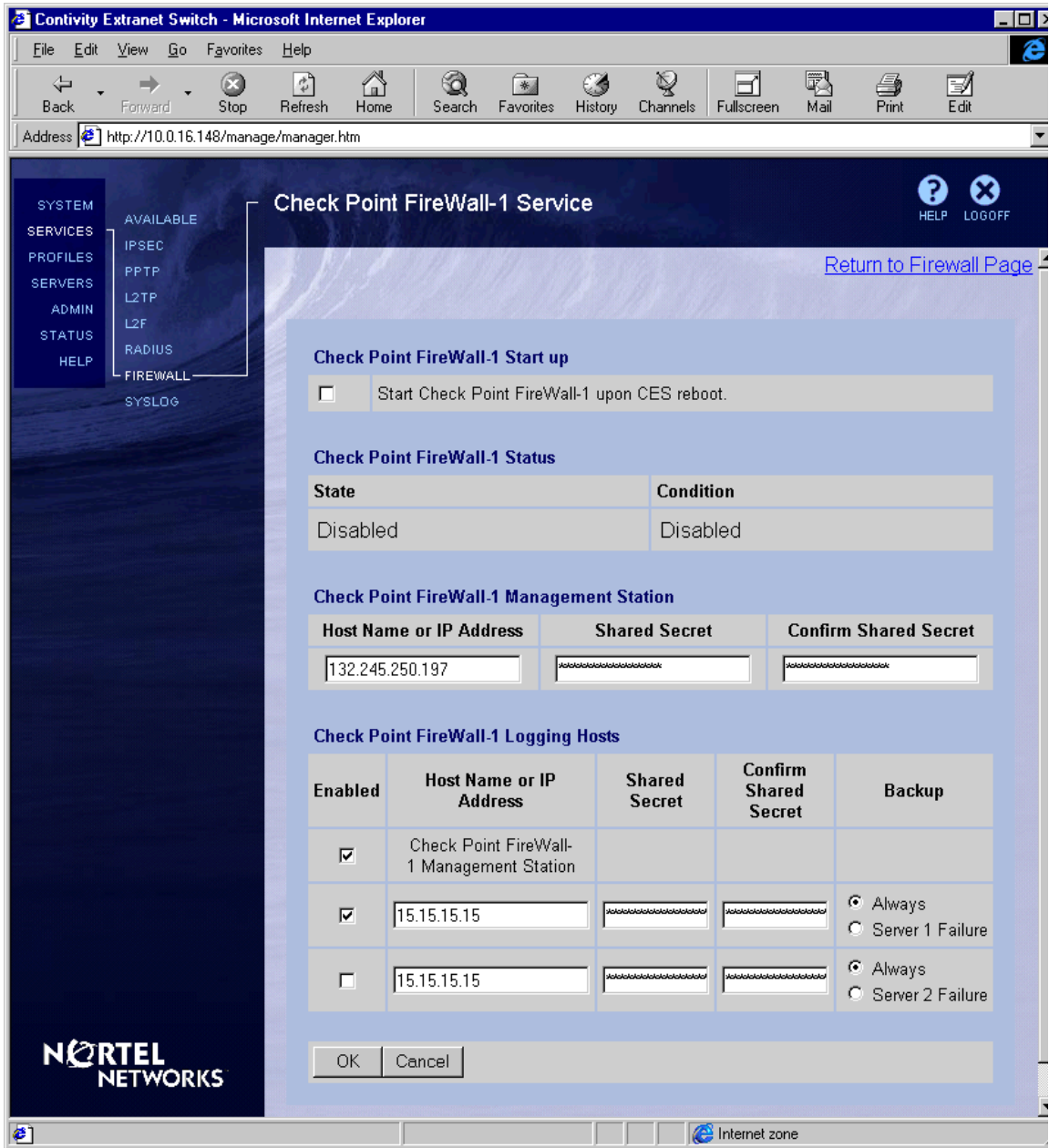
Contivity Tunnel Filter

When the check box is enabled, it allows you to use tunnel filters with the Stateful Firewall and migrate to the Stateful Firewall over time. You can build and test the Stateful Firewall policies while using the tunnel filters for traffic. Once you have the Stateful firewall policy set up (it has all of the same rules as the tunnel filters did), you can disable the tunnel filters and run the Stateful Firewall.

Check Point FireWall-1 Service

Use the Check Point FireWall-1 Service screen (Services→Firewall→Edit button) to start your Switch's integrated Check Point firewall and to manage the interaction between the firewall and the FireWall-1 Management Server.

Figure 39 Check Point FireWall-1 Service screen



The following sections describe the fields on the Check Point FireWall-1 Service screen.

Be sure that you click on the OK button to save any changes. After you click on OK, error messages appear at the top of this screen if required information is missing or incorrect.

Check Point FireWall-1 Start Up

Start Check Point FireWall-1 upon reboot

Use this check box to specify that you want the integrated Check Point firewall started when the Switch is rebooted. Make sure that you have also enabled the firewall by selecting Check Point on the Services→Firewall screen.

When the firewall is started, the Switch provides its enhanced routing capabilities. The enhanced routing is available as long as the Switch and the firewall are enabled.

Check Point FireWall-1 Status

State

Indicates the current status of the integrated Check Point firewall.

- Enabled indicates that the Start checkbox has been selected and the firewall has attempted to load. When the firewall is in the Enabled state, a Stop Check Point FireWall-1 button is displayed.
- Disabled indicates that the firewall could not load when you rebooted the Switch or that the Stop button was pressed.

Condition

Describes the condition that resulted in the firewall's current state. The possible conditions for each state are as follows:

Table 7 Check Point FireWall-1 states

State	Condition	Meaning
Enabled	Enabled	The firewall has loaded successfully and is up and running.
Enabled	Loading	The firewall has not completed the loading process. This might be caused by an incorrectly configured Management Station. This is an interim condition that eventually changes to either Enabled or Failure.
Disabled	Disabled	The firewall is not loaded or that you have pressed the Stop Check Point FireWall-1 button.
Disabled	Failure	The firewall unsuccessfully attempted to load and run.

Check Point FireWall-1 Management Station

This portion of the screen is used to identify and authenticate the Check Point FireWall-1 Management Station that manages the Switch's integrated firewall.

Although the FireWall-1 firewall is a component of the Switch, the firewall is set up and configured using a remote Firewall Management Station. The *Installing Check Point Firewall-1* book provides instructions for setting up your switch's firewall to create an efficient, yet secure environment. You should also refer to your Check Point FireWall-1 documentation for detailed firewall configuration instructions.

The integrated Check Point firewall must be running in order for the Management Station to gain access to it. You must also ensure that the Switch has been configured to accept management traffic from the firewall's Management Station. Refer to the first two rows in Table 8 for information.

Host Name or IP Address

The fully qualified domain name or IP address of the Management Station that you want to use to manage the firewall on the Switch.

Shared Secret

The shared secret between the Management Station and the Switch. The secret authorizes the Management Station to access and manage the Switch's firewall. The secret must be coordinated between you and the Management Station administrator.

Confirm Shared Secret

Reenter the shared secret to verify that you typed it correctly. You must define the integrated firewall as type switch on all Management Stations and firewall logging servers that you use.

Check Point FireWall-1 Logging Hosts

Logging hosts are machines to which the firewall writes its log file. As a means of providing backup to the logging information, you can specify multiple logging hosts.

Use the FireWall-1 Management Station GUI to display the log viewer on a selected logging host. The default log file is \$FWDIR/log/fw.log.

Enabled

Select the Enabled checkbox to specify that the log file is directed to the listed machine.

Host Name or IP Address

Enter either the fully qualified domain name or the IP address of the logging hosts.

Shared Secret

Enter the shared secret between the logging host and the Switch. Secrets must be coordinated between you and the administrator of the logging host.

Confirm Shared Secret

Reenter the shared secret to verify that you typed it correctly.

Backup

You can specify that the log file be sent to multiple logging hosts.

- Use the Always selection to specify that the log file is always sent to the listed logging host.
- Select the Server *n* Failure to specify that the log file is sent to the listed logging host only if Server *n* is not available.

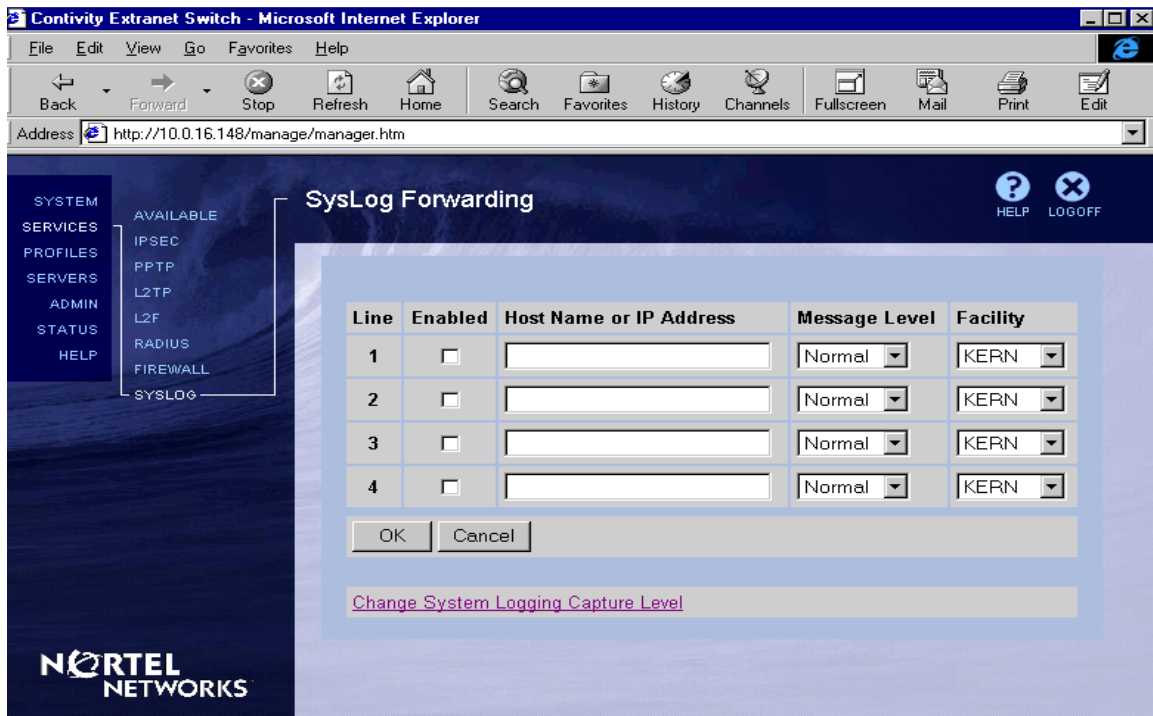
SysLog (System Forwarding)

System forwarding (Syslog) enables you to forward information from the system log to different host machines via the system logging daemon (syslogd). You can send different levels of information to different hosts. For example, you might send only Urgent system information to your primary system while sending “All” messages to a system you use for backup.



Note: The System Log (Status→System Log) setting has precedence over the Message Level you set on the Syslog Forwarding screen. For example, if you set Urgent on this Syslog Forwarding screen but Normal on the System Log screen, only Normal information is captured and available to Syslog Forwarding.

The section “System Log” provides additional information about system logging.

Figure 40 SYSLOG Forwarding

Enabled

Click to allow the Switch to send its system messages to the specific machine.

Host Name or IP Address

Enter either the fully qualified domain name or the IP address of the remote machine to which the log information is sent.

Message Level

The Message Level selection enables you to filter the information you send to the specified machines. For example, you might send Urgent system information to your primary system while sending All messages to systems you use for backup.

Urgent

Urgent Events are those that you want to be aware of immediately and that could potentially pose security or access problems; for example:

- Attempts to login with the wrong password.
- Attempts to gain Administrator Access.

Normal

Normal events are the everyday user and system interactions that allow you to review Switch activity; for example:

- Logins
- Configuration changes
- Scheduled or actual shutdowns

Detailed

Detailed events are designed specifically for use by Nortel Networks Customer Support personnel to uncover or troubleshoot problems.

All

The All selection is also designed specifically for Nortel Networks Customer Support personnel. This includes every log message that the system generates, including many details that are not of general interest but might allow Nortel Networks to uncover or troubleshoot problems.

Change System Logging Capture Level

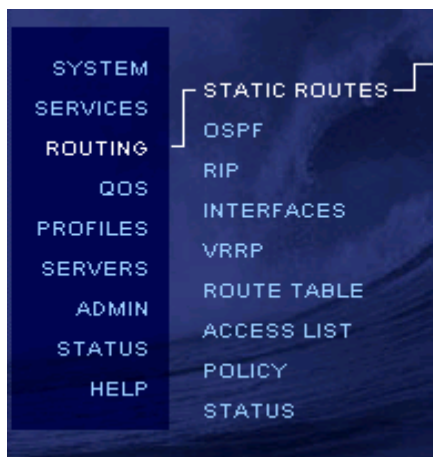
Click this link to go to the Status→System Log screen. At this screen you can specify the level of information you want to capture for the system log. Refer to the section “System Log” for a description of the System Log.

Chapter 3

Routing

The Routing menu provides access to screens that enable you to configure the various routing capabilities of the Switch.

Figure 41 Routing Menu



Static Routes

You can use static routes to set up routes between Switches when you do not have any dynamic routing protocol, such as OSPF or RIP. Even if you do have dynamic routing protocols, you may want to use static routes because they provide stronger security. The switch supports multiple default and static routes.

You can manually configure static routes on the switch. Based on their states, they are added or removed from the Route Table Manager (RTM). Click Routing→Static Routes to configure static routes.

Static Routes

Check the Enabled box to enable static routes. When this check box is cleared, all of the static routes and default routes are disabled globally. Even if a static route is enabled, the route is not used because the static routes are globally disabled. When static routes are enabled, traffic flow depends on other configuration settings.

Figure 42 Static Routes Configuration

Static Routes

Enabled ☒

OK Cancel

Default Routes

Type	Gateway Address	Interface	Admin State	Cost	Action
Private	10.0.0.10	LAN	Enabled	10	Edit Delete

Add Public Route Add Private Route

Static Routes through Physical Interfaces

IP Address	Subnet Mask	Gateway Address	Interface	Admin State	Cost	Action
Add						

Show Branch Office Routes

NORTEL NETWORKS

Default Routes

In the absence of any defined route, packets are forwarded to the gateway specified as the default route. These default routes can be either private or public static routes. Private routes are available whether or not a firewall is enabled. Public routes are available only if an integrated firewall is enabled.

A private default static route is the default route used for traffic that comes into the Switch from a private interface. Incoming traffic uses the private default route when there is no public default route defined. If you do not define either a public or private default route, the traffic is dropped. When you add a private default route, the route table adds a new static route.

A public default static route is the default route used for traffic that comes into the Switch from a public interface or through a tunnel. If you do not define a public default route, the traffic is dropped. When you add a public default route, a new static route is added to the route table. You can configure multiple default routes to the same destination with different gateways.

Type

Shows whether the static route is Public or Private.

Gateway Address

Address where packets are routed onto the network.

Interface

Shows whether the default route is a LAN or WAN interface.

Admin State

Shows whether the route is enabled or disabled.

Cost

Shows the relative cost for the switch. You would use a lower cost number, such as 1, for the least expensive route. When there are multiple default paths, the switch chooses the route with the least cost as the preferred route. The default is 10.

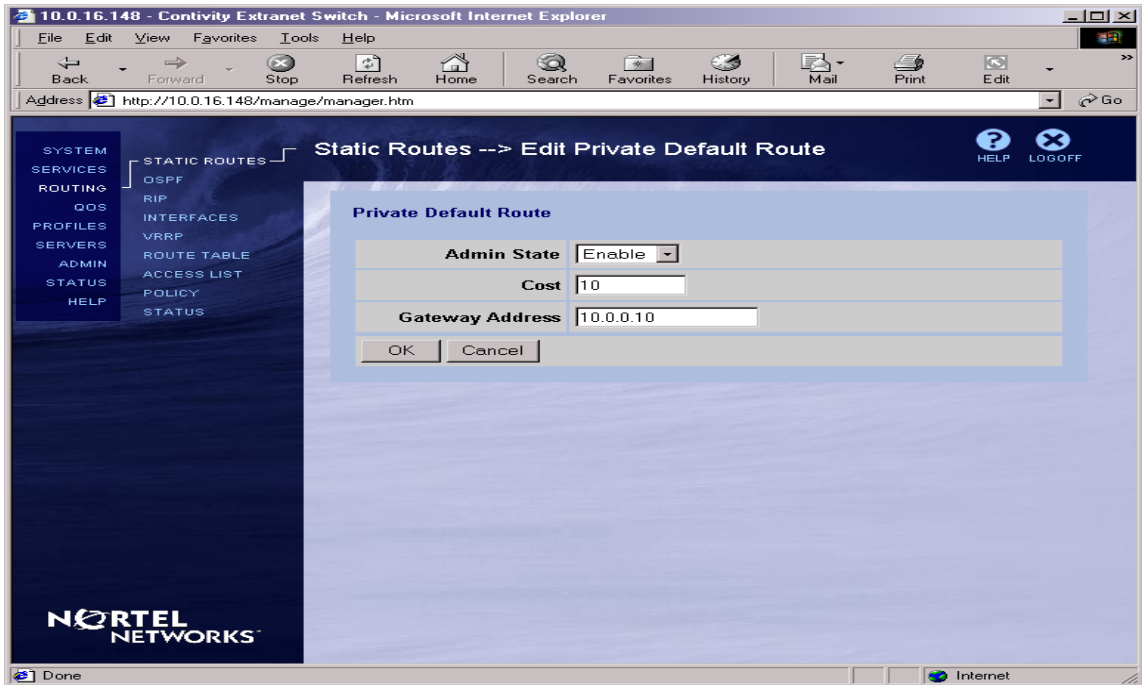
Action

Click on the appropriate buttons to edit or delete default routes.

Edit

To edit an existing default static route, click on the edit button in the Action column. The Static Routes → Edit screen appears with display of the appropriate information about that route. Select Enable or Disable from the Admin State dropdown list. Type in the cost in the Cost edit box and the gateway address in the Gateway Address edit box.

Figure 43 Static Routes → Edit

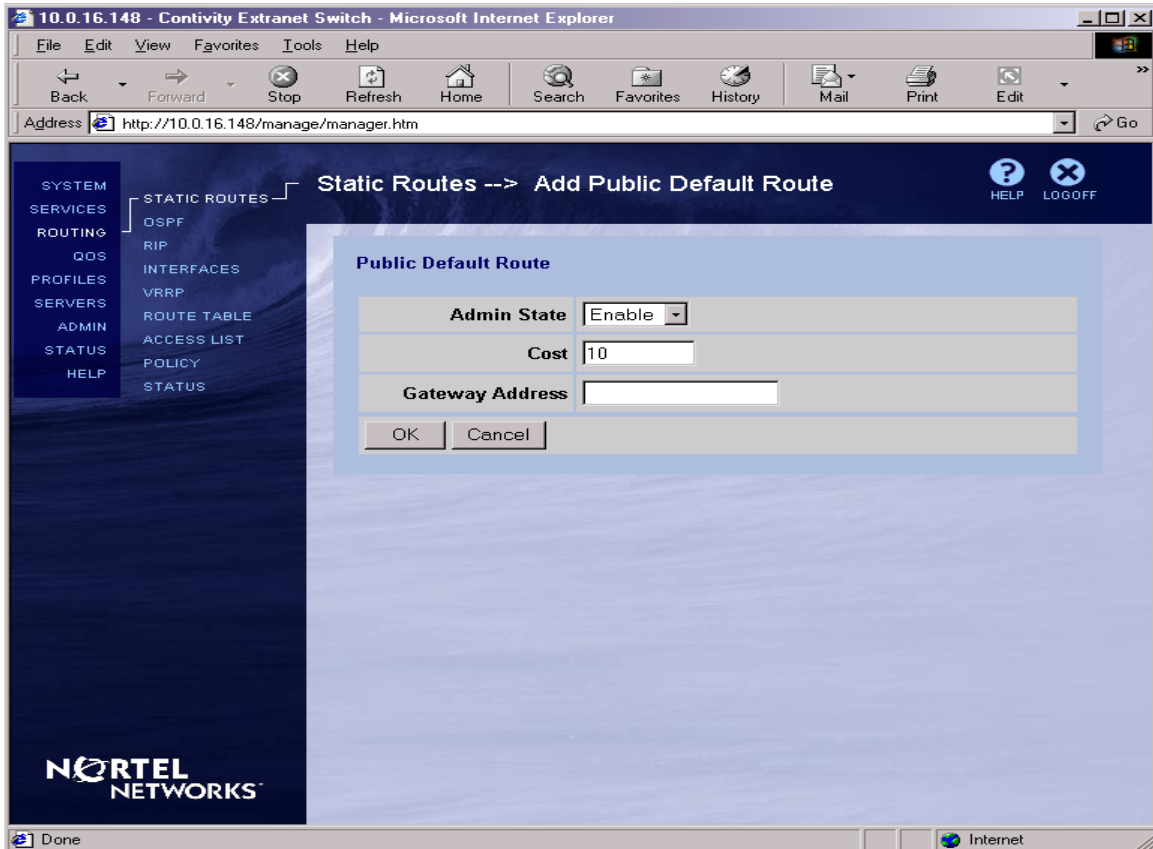


Delete

Click on the Delete button to delete the default static route.

Add Public Route

To edit a default public static route, click on the edit button in the Action column. The Static Routes → Add Public Default Route screen appears with display of the appropriate information about that route. Select Enable or Disable from the Admin State dropdown list. Type in the cost in the Cost edit box and the gateway address in the Gateway Address edit box.

Figure 44 Static Route→Add Public Default Route screen

Add Private Route

To add a default private route, click on the edit button in the Action column. The Static Routes→Edit screen appears with a display of the appropriate information about that route. Select Enable or Disable from the Admin State drop down list. Type in the cost in the Cost edit box and the gateway address in the Gateway Address edit box.

Figure 45 Static Routes→Add Private Default Route

The screenshot shows the Nortel Networks configuration interface. On the left is a dark blue sidebar with a menu containing: SYSTEM, SERVICES, ROUTING, QOS, PROFILES, SERVERS, ADMIN, STATUS, and HELP. The 'ROUTING' menu item is expanded, showing a sub-menu with: STATIC ROUTES, OSPF, RIP, INTERFACES, VRRP, ROUTE TABLE, ACCESS LIST, POLICY, and STATUS. The 'STATIC ROUTES' menu item is selected, and the main window title is 'Static Routes --> Add Private Default Route'. In the top right corner of the main window are 'HELP' and 'LOGOFF' buttons. The main content area is titled 'Private Default Route' and contains a form with the following fields: 'Admin State' with a dropdown menu set to 'Enable', 'Cost' with a text box containing '10', and 'Gateway Address' with an empty text box. At the bottom of the form are 'OK' and 'Cancel' buttons. The Nortel Networks logo is in the bottom left corner of the sidebar.

Static Routes through Physical Interfaces

This section displays a list of all configured static routes (through any physical interface). A static route differs from a default static route in that it specifies a particular destination, such as an IP subnet or an IP host, represented by the IP address and subnet mask. You can configure multiple static routes to the same destination with a different next hop gateway and with the same or different costs.

IP Address

IP address of the static route for the destination network.

Subnet Mask

Subnet mask for the static route for the destination network.

Gateway Address

Address where packets are routed for the destination network.

Interface

Shows whether the default route is a LAN or WAN interface. The default is LAN.

Admin State

Shows whether the route is enabled or disabled. The default is enabled.

Cost

Shows the relative cost for the switch. You would use a lower cost number (for example, 1) for the least expensive route. When there are multiple paths, the switch chooses the route with the least cost as the preferred route. The default is 10.

Action

Click on the appropriate buttons to add, edit, or delete default routes.

Edit

To edit an existing static route, click on the edit button. The Static Routes→Edit Static Route screen appears with a display of the appropriate information about that route. Select Enable or Disable from the Admin State drop down list. Type in the cost in the Cost edit box and the gateway address in the Gateway Address edit box.

Figure 46 Static Routes→Edit Static Route

The screenshot shows the 'Static Routes -> Edit Static Route' configuration window in the Nortel Networks management interface. The left sidebar contains a menu with options: SYSTEM, SERVICES, ROUTING, QOS, PROFILES, SERVICES, ADMIN, STATUS, and HELP. The 'ROUTING' section is expanded, showing sub-options: STATIC ROUTES, RIP, INTERFACES, VRRP, ROUTE TABLE, ACCESS LIST, POLICY, and STATUS. The 'STATIC ROUTES' option is selected. The main window displays the 'Static Route' configuration form with the following fields:

Field	Value
Admin State	Enable
Cost	10
Network Address	10.0.0.140
Subnet Mask	255.255.255.255
Gateway Address	10.0.0.2

At the bottom of the form are 'OK' and 'Cancel' buttons. The Nortel Networks logo is visible in the bottom left corner of the interface.

Delete

Click on the Delete button to delete the static route.

Add Route

Click on the add button to add static routes to the routing table. The Static Routes→Add screen appears. When a static route is added, the switch checks whether the next hop interface address belongs to an attached network. If it does not, the switch does not allow such static routes.

Figure 47 Static Routes→Add Static Route screen

SYSTEM
SERVICES
ROUTING
QOS
PROFILES
SERVERS
ADMIN
STATUS
HELP

STATIC ROUTES
OSPF
RIP
INTERFACES
VRRP
ROUTE TABLE
ACCESS LIST
POLICY
STATUS

Static Routes --> Add Static Route

HELP LOGOFF

Static Route

Admin State: Enable

Cost: 10

Network Address:

Subnet Mask:

Gateway Address:

OK Cancel

NORTEL NETWORKS

Admin state

Shows whether the route is enabled or disabled. The default is enabled.

Cost

Shows the relative cost for the switch. You would use a lower cost number (for example, 1) for the least expensive route. When there are multiple paths, the switch chooses the route with the least cost as the preferred route. The default is 10.

Network address

IP address of the static route for the destination network.

Subnet mask

Subnet mask for the static route for the destination network.

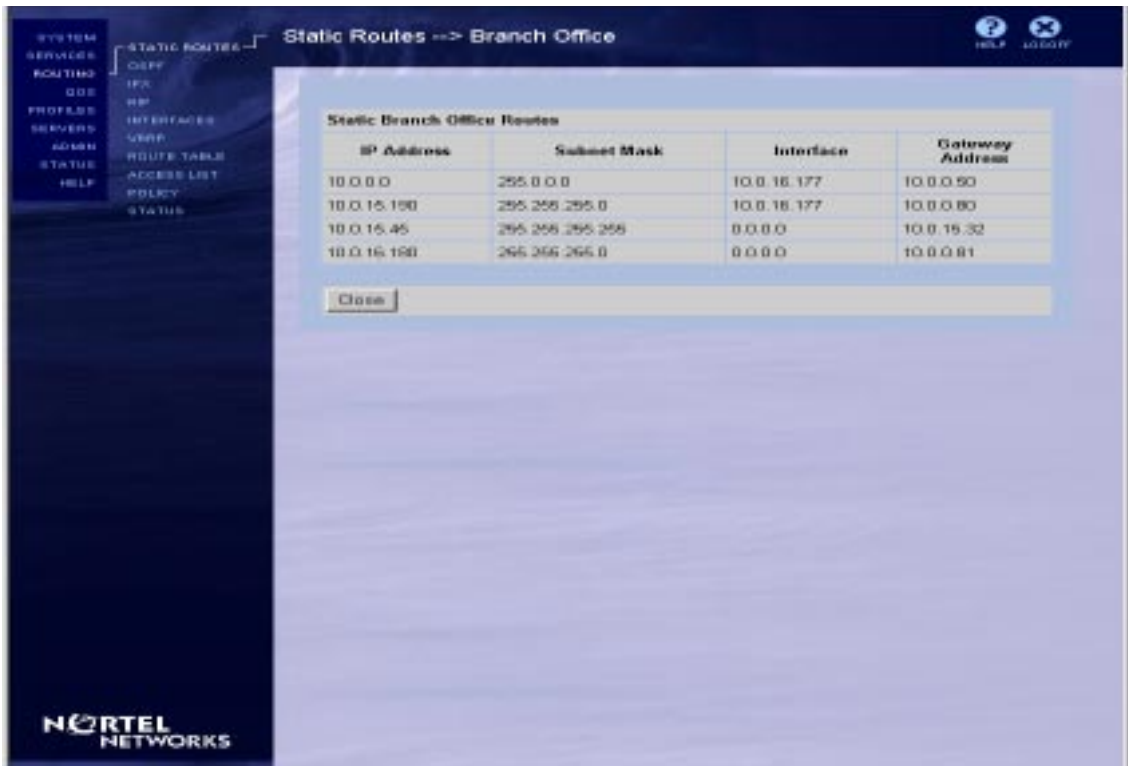
Gateway address

Address where packets are routed for the destination network.

Show Branch Office Routes

This screen shows the configured Branch Office tunnels that are set up as static routes. By default, a tunnel is configured as a static route between the tunnel end points.

Figure 48 Static Routes→Branch Office



IP Address	Subnet Mask	Interface	Gateway Address
10.0.0.0	255.0.0.0	10.0.16.177	10.0.0.90
10.0.15.190	255.255.255.0	10.0.16.177	10.0.0.80
10.0.15.45	255.255.255.255	0.0.0.0	10.0.15.32
10.0.15.190	255.255.255.0	0.0.0.0	10.0.0.81

Close

NORTEL NETWORKS

IP address

IP address of the branch office route.

Subnet mask

Subnet mask of the branch office route.

Interface address

Local IP address of the branch office interface.

Gateway address

Remote peer address where packets are routed onto the network.

Admin State

Enabled or disabled. To edit this field, go to Branch Office→Edit→IP and click on Add Route under the Static Route section.

Cost

Shows the relative cost for the switch. You would use a lower cost number, such as 1, for the least expensive route. If the number is more than 1, the lowest cost is the preferred number. To edit this field, go to Branch Office→Edit→IP and click on Add Route under the Static Route section.

OSPF

OSPF (Open Shortest Path First) is a link-state routing protocol that maintains a database from which a routing table is constructed from the shortest path, using a minimum of routing protocol traffic. It provides a high functionality open protocol that allows multiple vendor networks to communicate using the TCP/IP protocol family. Some of the benefits of OSPF are:

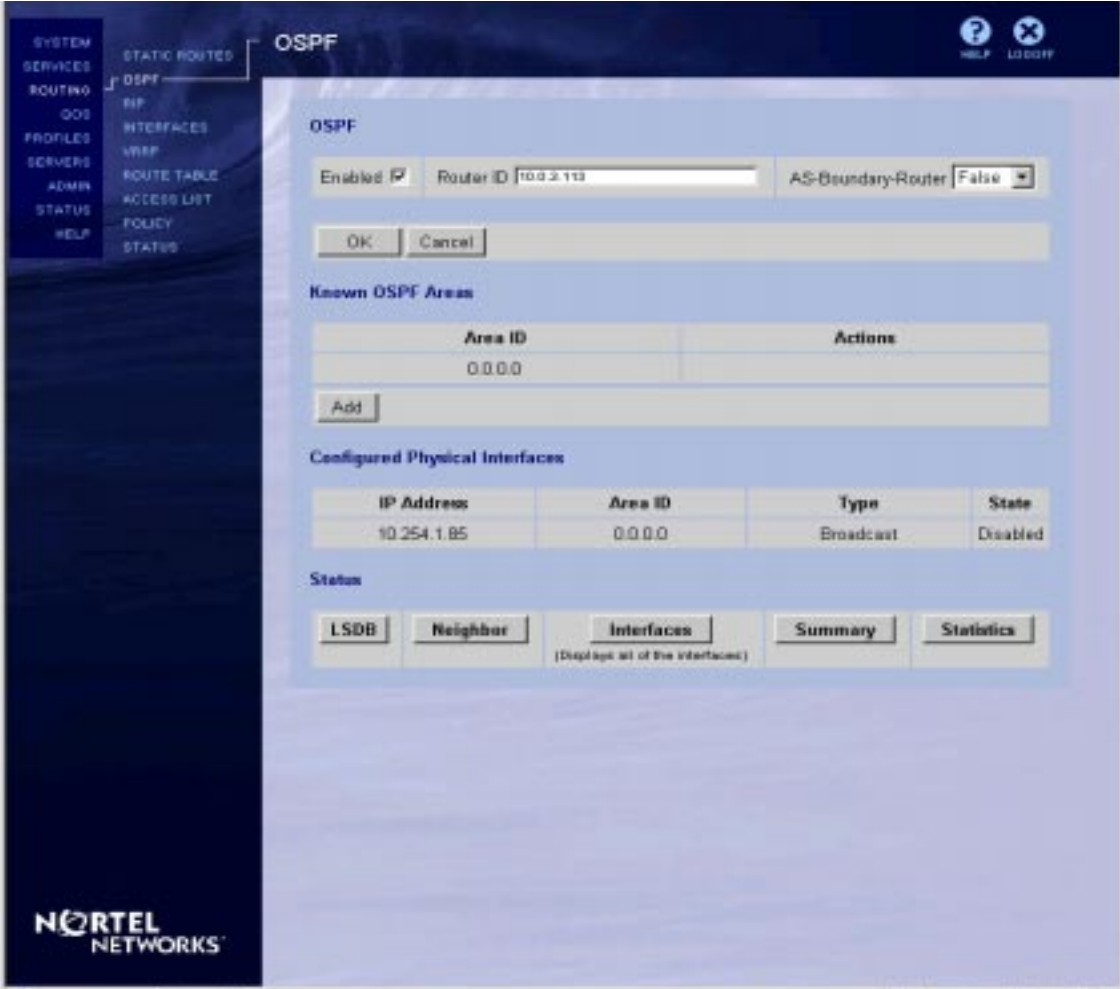
- Fast convergence

- Variable Length Subnet Masks (VLSM)
- Hierarchical segmentation
- Area routing to provide additional routing protection and a reduction in routing protocol traffic
- Authentication

OSPF Configuration

Click Routing→OSPF to configure OSPF global parameters.

Figure 49 Routing→OSPF



Enabled

Indicates that the OSPF protocol is enabled on this screen. The default setting is disabled.

Router ID

Type in the IP address in the Router ID field. This uniquely identifies the router in an area and defaults to the lowest of the IP addresses of management/physical interfaces defined in the switch. You can change this address provided that it is unique within the area. The default is the lowest IP interface in the box.

AS-Boundary-Router

An AS-Boundary-Router is a router that exchanges routing information with routers belonging to other autonomous systems and advertises AS external routing information throughout the AS. To configure the switch as an Autonomous System Boundary Router, select True from the AS-Boundary-Router drop down list. The default is false. This parameter must be set to True if you want to enable redistribution of non-OSPF routes via OSPF.

Known OSPF Areas

This section displays all of the OSPF areas defined locally to the switch. The area information is not shared among Switches. If you want two Switches to have one of their interfaces in a common area, you must configure both Switches to define the area information.

Area ID

Area IDs are used as representations of parts of the OSPF network. They help to manage large numbers of networks so that they can exchange information within an area. Each Area ID must be unique for OSPF. By default all Switches have an area named 0.0.0.0.

Add

To add an OSPF area, click on the add button. The Routing Protocols→Add Area screen appears.

Area ID

List the ID of the area that you want to edit.

Stub

Select True or False from the drop-down list. The default is False.

Stub Metric

Type in the number of the stub metric. The default is 1.

Edit

When you add an area, you can edit the information for that area by clicking on the Edit button next to the area. The OSPF→Edit Area screen appears. You can change the information for the Area ID, Stub and Stub Metric as explained above. You can also delete an existing area range or add an area range.

Figure 50 Routing→OSPF→Edit Area

The screenshot shows the 'OSPF --> Edit Area' configuration window. On the left is a navigation menu with options like SYSTEM, SERVICES, ROUTING, QOS, PROFILES, SERVERS, ADMIN, STATUS, and HELP. The main area is titled 'OSPF Area' and contains the following fields:

- Area ID:** 1.1.1.1
- Stub:** False (dropdown menu)
- Stub Metric:** 1

Below these fields is the **Area Range** section, which shows a list of ranges with a 'Delete' button next to the selected range '1.0.0.0 - 255.255.0.0'. At the bottom is the **Add an Area Range** section, which includes input fields for 'IP Address' and 'Mask', an 'Add' button, and 'OK' and 'Cancel' buttons at the very bottom.

Area Range

The edit box lists all existing area ranges. Select the area range and click the Delete button to delete the range.

Add an Area Range

In the edit boxes, type in the IP address and subnet mask of the area range that you want to specify.

Configured Physical Interfaces

IP address

IP address of the configured OSPF interfaces. The default is 0.0.0.0.

Area ID

Area ID of the configured OSPF interfaces. The default is 0.0.0.0.

Type

Broadcast or Point-to-Point. The default is Broadcast.

State

Enabled or disabled. The default is enabled.

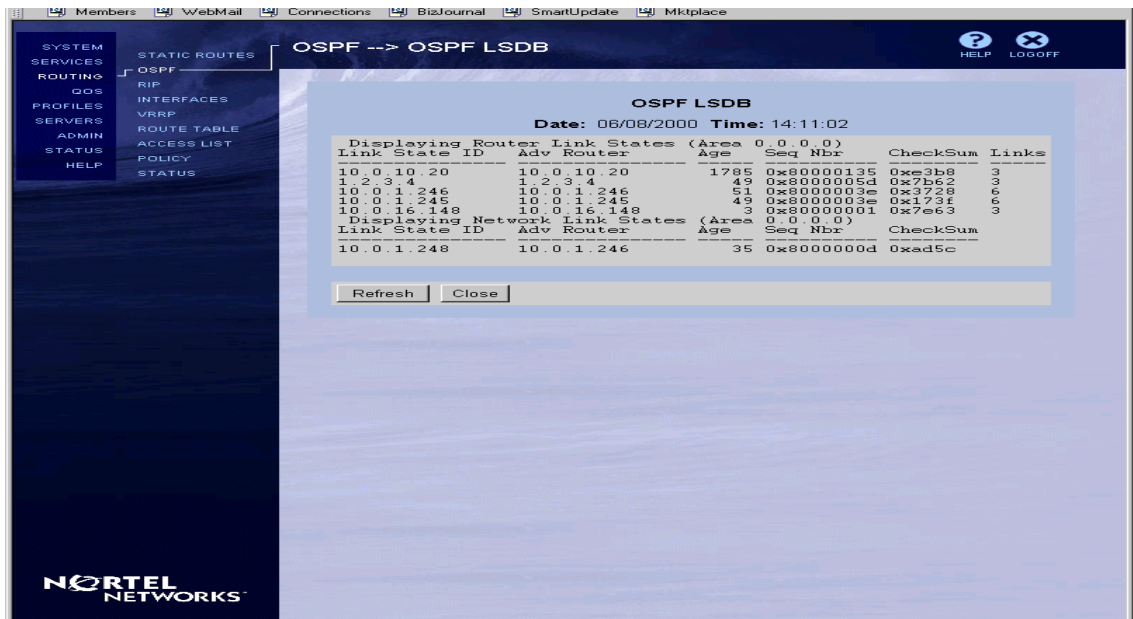
Status

This section allows you to display. OSPF LSDB (Link State Database), Neighbor, Interfaces, or Summary.

OSPF LSDB

When you click on the LSDB button, the screen lists the link state databases in all areas that are configured in that switch.

Figure 51 Routing→OSPF→LSDB



The following table describes the information in the OSPF LSDB screen.

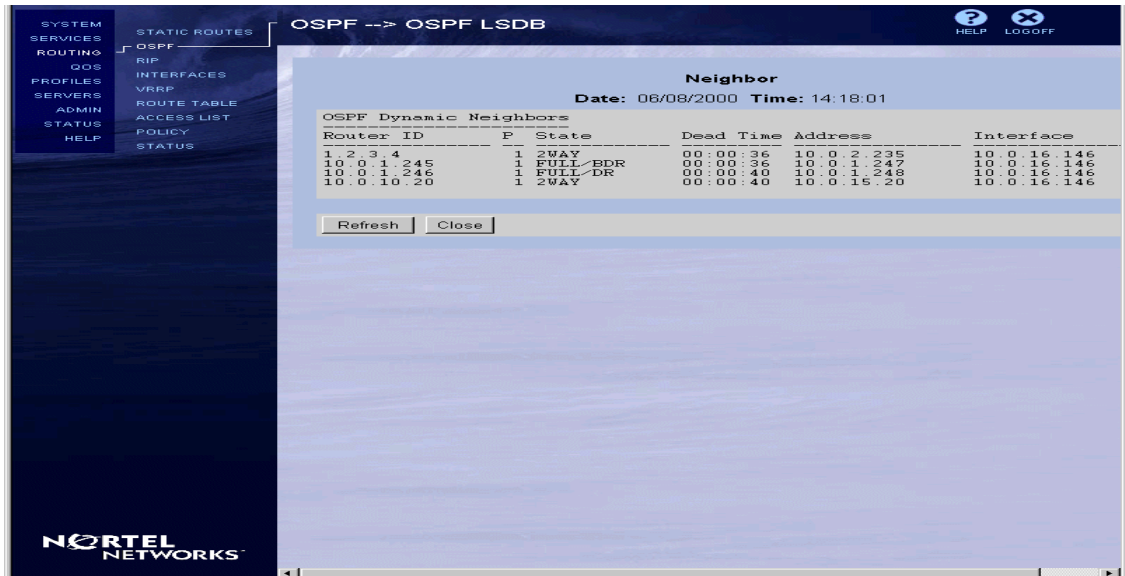
Table 8 OSPF LSDB

Column	Description
Link State ID	Link state address
Adv Router	Advertising router address
Age	Age in seconds
Seq Nbr	Sequence number
CheckSum	Checksum
Links	Number of links

Neighbor

When you click on the Neighbor button, the screen shows the list of neighbors on all the interfaces running OSPF.

Figure 52 Routing→OSPF→Neighbor



The following table describes information on the OSPF Neighbors screen.

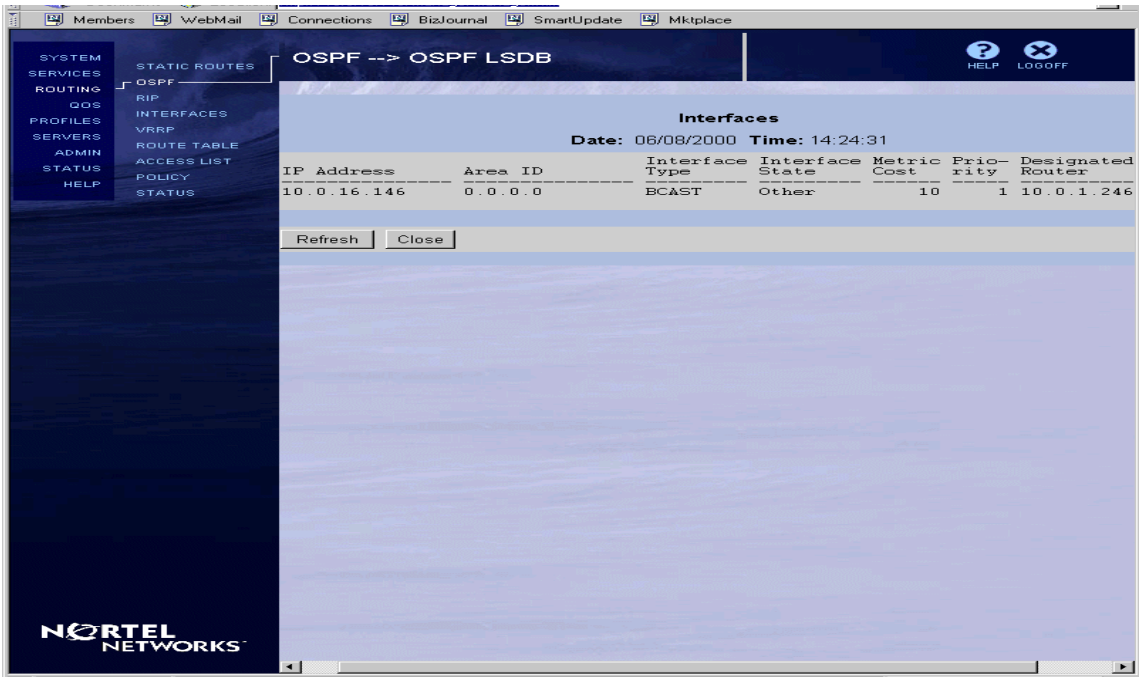
Table 9 OSPF Dynamic Neighbors

Column	Description
Router ID	OSPF ID of neighbor
P	Priority number
State	State of neighbor connection
Dead Time	Time until neighbor is declared dead
Address	Neighbor IP address
Interface	Local IP interface address

Interfaces

When you click on the Interfaces button, the screen shows the list of interfaces that you configured for OSPF.

Figure 53 OSPF→Interfaces screen



The following table describes the fields for the OSPF Interfaces screen.

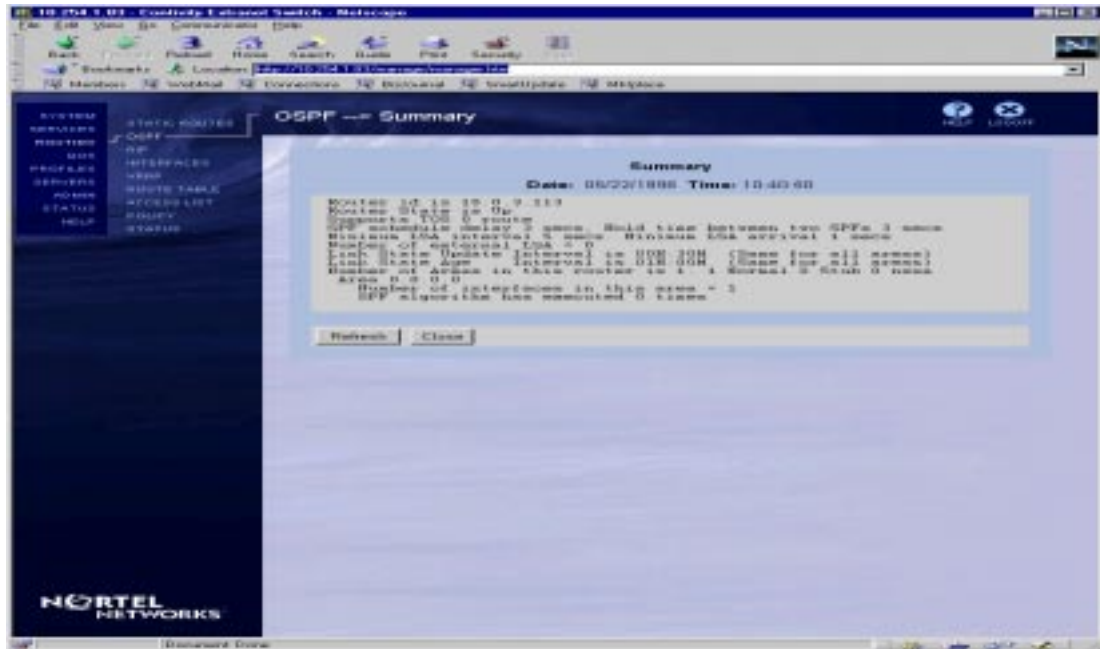
Table 10 OSPF interfaces

Column	Description
IP Address	Local IP address
Area ID	OSPF area for the interface
Interface Type	Broadcast (BCAST) for Point to Point (PTPT)
Interface State	State of interface: Enabled or Disabled (physical) or Other (tunnel)
Metric Cost	Cost associated with the interface
Priority	Priority used to negotiate DR/BDR state
Designated Router	Designated router (0.0.0.0 for PTPT)

Summary

When you click on the Summary button, the screen shows the overall summary of OSPF running on the switch.

Figure 54 OSPF→Summary



The following table describes fields on the OSPF Summary screen.

Table 11 OSPF Summary

Column	Description
Router ID	Unique OSPF ID of router
Router State	OSPF global configured state (up or down)
Supports TOS	Type of Service support
SPF schedule delay	Shows Shortest Path First
Hold time between two SPF's	Time between Shortest Path First calls
Minimum LSA interval	Link state advertisement interval
Minimum LSA arrival	Link state advertisement arrival minimum

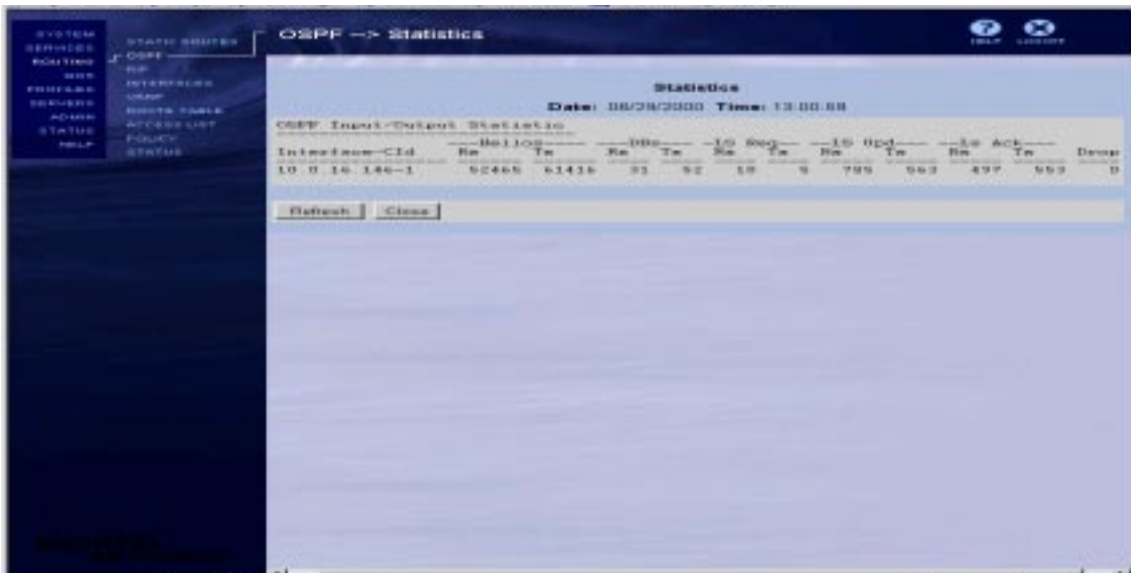
Table 11 OSPF Summary

Column	Description
Number of external LSA	Number of link state advertisements
Link State Update Interval	Time between link state updates
Link State Age Interval	Time between link state age intervals
Number of Areas in this router	Number of areas
Area	Area ID
Number of interfaces in this area	Number of interfaces in this area
SPF algorithm has executed	Number of times shortest path algorithm has been executed

Statistics

When you click on the Statistics button, the system displays statistical information about OSPF.

Figure 55 OSPF→Statistics



The following table describes the fields on the OSPF Statistics screens.

Table 12 OSPF Statistics

Column	Description
Interface-CID	Local IP interface address and circuit ID
Hellos	Number of “Hello” packets received and transmitted
DBs	Number of “DB” (Database Exchange) packets
LS Req	Link state requests
LS Upd	Link state updates
LS Ack	Link state acknowledgements

RIP

The Routing Information Protocol (RIP) is a distance-vector routing protocol that enables routers to exchange routing information by means of periodic RIP updates. Routers transmit their own RIP updates to neighboring subnets and listen for RIP updates from the routers on those neighboring subnets. Routers use the information in the RIP updates to keep their internal routes current.

For RIP, the “best” path to a destination is the path with the fewest hops. RIP computes distance as a metric, usually the number of hops (or routers) from the origin subnet to the target subnet. RIP can handle a maximum of 15 hops.

Figure 56 RIP

RIP

Enabled ☐ Update Timer (seconds)

OK Cancel

Configured Physical Interfaces

IP Address	State
10.0.16.146	Enabled

Status

Statistics Database Interfaces
(Displays all of the interfaces)

NORTEL NETWORKS

Enabled

Check the Enabled check box to enable RIP on the Switch. By default RIP is globally disabled. If RIP is disabled on this screen, the switch does not process any RIP requests. After you enable RIP on this screen, you must also enable it on the Routing→Interfaces screen.

Update Timer

In the Update Timer edit box, enter the amount of time in seconds that you want RIP to update the routes. The default is 30 seconds. The range of values that you can specify is from 5 seconds to 65535 seconds. The hold down timer is six times the update timer. Routes are invalid after the time set on the hold down timer.

Configured Interfaces

IP Address

IP address of the RIP interface.

State

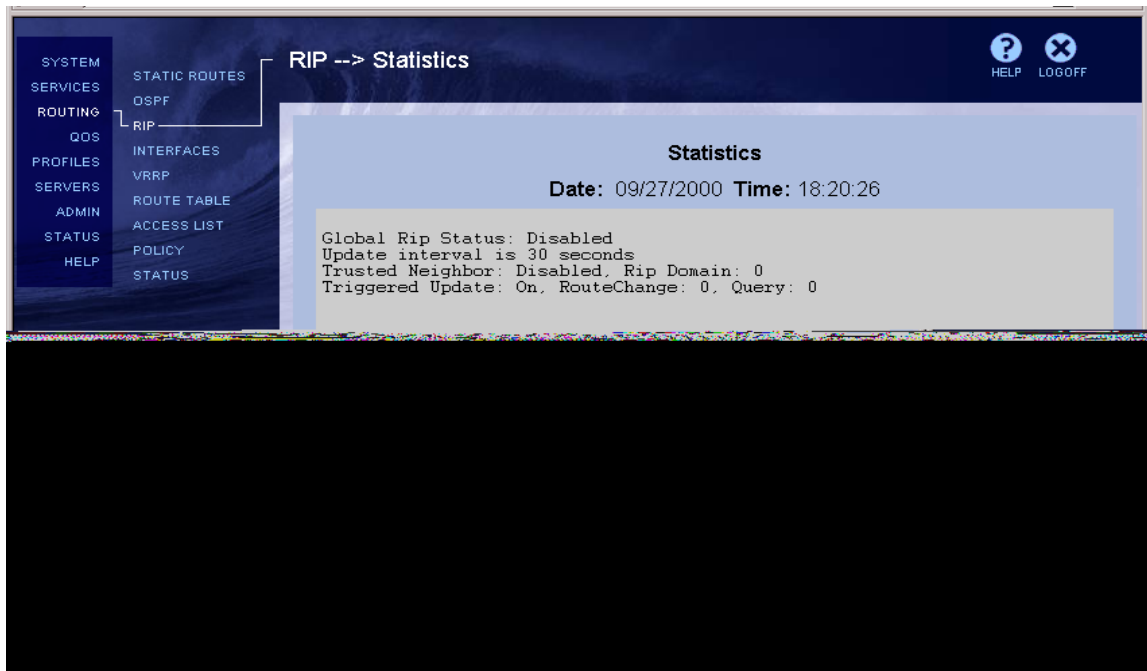
Whether the RIP protocol is enabled or disabled on this interface.

Status

Statistics

Displays statistics about the RIP protocol in the switch.

Figure 57 RIP→Statistics



The following table describes the fields on the RIP Statistics screen.

Table 13 RIP statistics

Column	Description
Global RIP Status	Enabled or disabled
Update interval	Interval in seconds

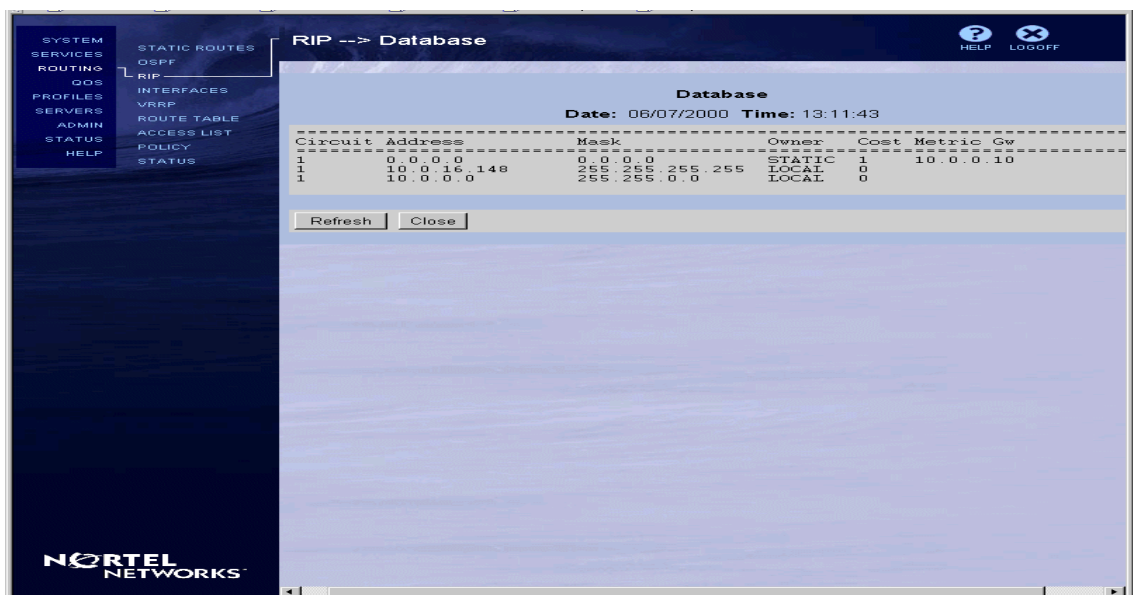
Table 13 RIP statistics

Column	Description
Trusted Neighbor	Enabled or disabled
Rip Domain	Set or reset
Triggered Update	Set or reset
Route Change	Number of routes changed
Query	Number of queries sent

Database

Displays information for all of the RIP interfaces.

Figure 58 RIP database



The following table describes the fields on the RIP Database screen.

Table 14 RIP database

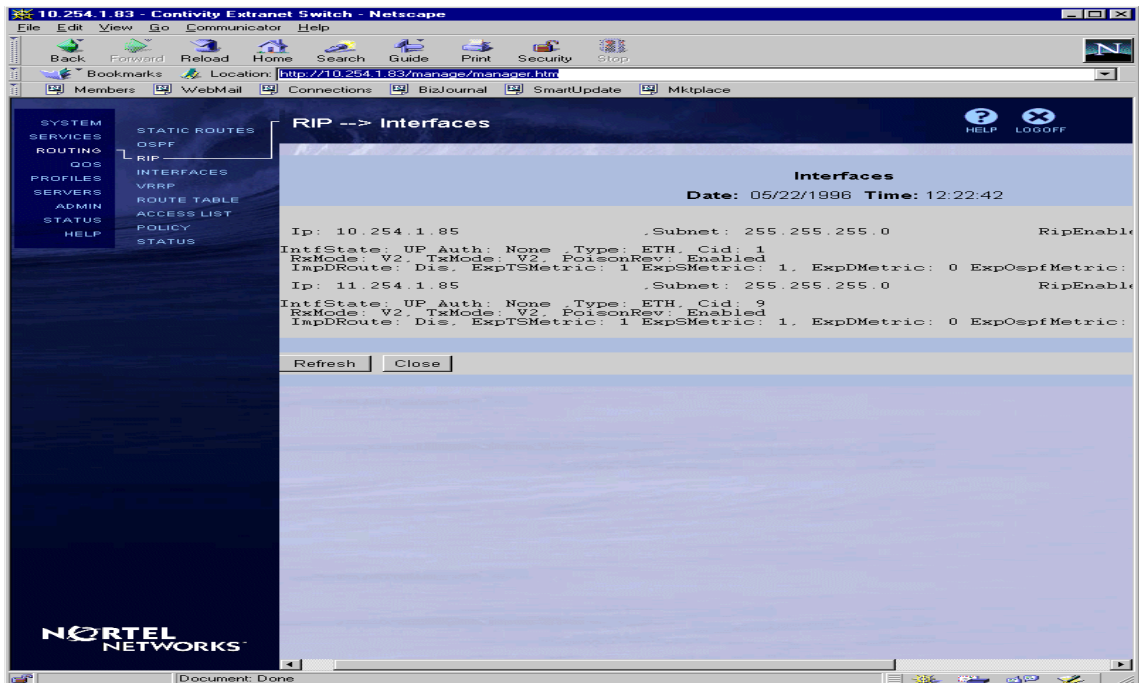
Column	Description
Circuit	Circuit ID
Address	IP address

Table 14 RIP database

Column	Description
Mask	Network mask of IP address
Owner	Protocol
Cost	Import cost of RIP routes
Metric	Export metric of RIP routes
Gw	Gateway IP address

Interfaces

Displays information for all of the RIP interfaces, including tunnels that are running RIP.

Figure 59 RIP→Interfaces

The following table describes the fields on the RIP Interfaces screen.

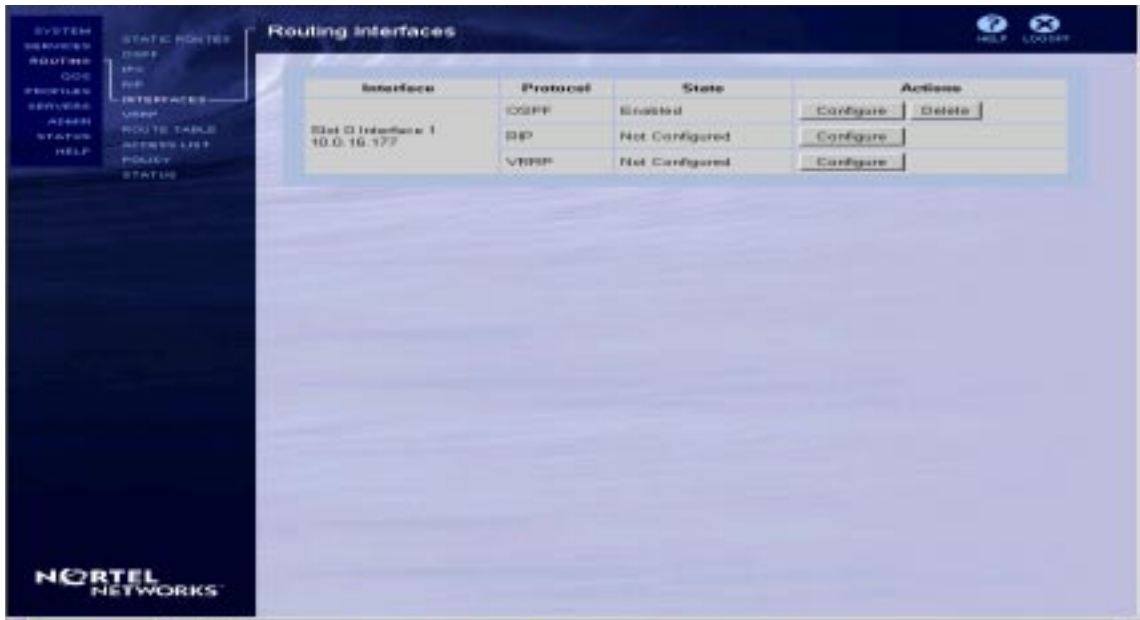
Table 15 RIP Interfaces

Column	Description
Ip	RIP IP address
Subnet	Network mask of IP address
RipEnabled	Whether RIP is enabled or disabled
IntfState	Whether up or down
Auth	Authentication type
Type	Interface type
Cid	Circuit ID
RxMode	RIP receive version supported
TxMode	RIP transmit version supported
PoisonRev	Whether enabled or disabled
ImpDRoute	Whether enabled or disabled
ExpTSMetric	Disabled or metric (1-15) export tunnel static route
ExpSMetric	Disabled or metric (1-15) export static route
ExpDMetric	Disabled or metric (1-15) export default route
ExpOspfMetric	Disabled or metric (1-15 export OSPF route

Interfaces

The Interfaces screen allows you to choose the routing interface that you want to configure. The supported routing protocols are OSPF, RIP, and VRRP.

Figure 60 Routing Interfaces



Physical interface

Slot number, interface number, and corresponding IP address.

Protocol name

OSPF, RIP or VRRP.

State

Enabled, Disabled, or Not configured. The default reflects the configured state.

Actions

Configure, Delete or Disable/Enable.

OSPF

When you click on the Configure button under the Actions Section for OSPF, the Configure OSPF screen appears.

Figure 61 Routing Interfaces→Configure OSPF

The screenshot displays the 'Routing Interfaces → Configure OSPF' configuration page in the Nortel Networks web interface. The left sidebar contains a navigation menu with options: SYSTEM, SERVICES, ROUTING, PROFILES, SERVERS, ADMIN, STATUS, and HELP. The 'ROUTING' section is expanded, showing sub-options: STATIC ROUTES, OSPF, IPX, RIP, INTERFACES, VRRP, ROUTE TABLE, ACCESS LIST, POLICY, and STATUS. The 'INTERFACES' option is selected.

The main configuration area is titled 'Routing Interfaces → Configure OSPF' and contains the following fields and options:

- Interface:** Slot 0 Interface 1
- IP Address:** 10.0.16.177
- State:** Enabled (dropdown menu)
- Area ID:** 0.0.0.0 (dropdown menu) with a link to [Add an Area ID](#)
- Type:** Broadcast (dropdown menu)
- Authentication:** none (dropdown menu)
- Cost:** 10
- Priority:** 1
- Hello Interval:** 10
- Dead Interval:** 40 (Note: (Dead interval value must be at least 4 times Hello interval))
- Poll Interval:** 120 (Note: (Polling interval value must be greater than Hello interval))
- Retransmission Interval:** 5
- Transmission Delay:** 1

At the bottom of the configuration area are 'OK' and 'Cancel' buttons. The Nortel Networks logo is visible in the bottom left corner of the interface.

Interface

Interface number and slot.

IP Address

IP address of the interface.

State

State of OSPF, either enabled or disabled. The default is enabled.

Area ID

OSPF area to which the attached network belongs. The default is 0.0.0.0.

Type

OSPF network type, such as Broadcast or Point-to-Point. The default is Broadcast.

Authentication

OSPF authentication type, such as Simple, MD5, or none. If you select Simple, you need to supply a password and confirm it. If you select MD5, you must supply the Secret and confirm it. The default is none.

Cost

Cost of sending a packet on the interface expressed in the link state metric. Must always be greater than 0. The default is 10.

Priority

Priority of the routers on this interface. The router with the highest priority takes precedence in determining which is the designated router (DR). If there is a tie, the router with the highest Router ID takes precedence. A priority setting of 0 is ineligible to become a designated router on the attached network. Router priority only applies to broadcast networks. The default is 1.

Hello Interval

Length of time in seconds between the Hello packets that the router sends on the interface. It must be the same for all routers attached to a common network. The default is 10.

Dead Interval

Number of seconds after a router ceases to hear Hello packets before declaring that the router is down. It must be the same for all routers attached to a common network. The default is 40.

Poll Interval

If a neighboring router becomes inactive, the router sends packets at a reduced rate in seconds. The default is 120.

Retransmission Interval

Number of seconds between LSA retransmission for adjacencies belonging to this interface. It is also used for retransmitting Database Description and Link State Request packets. This setting should be considerably over the expected round trip delay between any two routers on the attached network, and should be conservative to prevent needless retransmissions. The default is 5.

Transmission Delay

Estimated number of seconds it takes to transmit a Link State Update Packet over this interface. The default is 1.

RIP

To change the RIP configuration, go to Routing Interfaces→Configure RIP screen.

Figure 62 Routing Interfaces→Configure RIP

Enabled

Indicates that the RIP specifications on this interface have been enabled. (You have selected the global Enabled specification on the Routing→RIP screen.) The default is Enabled.

Transmit Mode

Transmit Mode enables you to specify which version of the RIP protocol is used when routing traffic from this Switch. The default of V2 indicates RIP-2. You can select V1 to specify that RIP-1 traffic is sent. A selection of OFF specifies that RIP is not used.

Receive Mode

Receive Mode enables you to specify which version of the RIP protocol the Switch accepts for incoming traffic. The default of V2 indicates that only RIP-2 traffic is accepted. You can select V1 to specify that RIP-1 is accepted. If you select OFF, RIP traffic is not accepted. If you select BOTH, incoming transmissions using either version of RIP are accepted.

Authentication

Indicates the type of authentication that is used as part of the RIP transmission. This authentication is specific to the RIP routing protocol and has no bearing on the authentication done as part of the connection to the Switch. The default is None, which specifies that no authentication is required.

SIMPLE indicates that authentication is accomplished by using a simple password. MD5 specifies that authentication is accomplished by using a MD5 secret. If you select either Simple or MD5, password and confirmation fields are displayed below the selection.

Poison Reverse

Click to enable or disable poison reverse. Poison reverse updates remove routing loops in large networks.

Import Default Route

Typically, you specify a default route in the Switch's Routing Table using Routing→Static routes. The Switch then uses that default route when sending traffic to the private/public network. However, if no default route has been set, you can check the Import Default Route box and the Switch uses the default route that it learned during RIP updates. The default is disabled.

Export Default Routes Metric

Use this field to specify that the Switch's default route is exported during RIP updates. You can also choose a metric value (1 through 15) to the default route. The default is disabled.

Export Static Routes Metric

Use this field to specify that the Switch's static routes are exported during RIP updates. You can also choose a metric value (1 through 15) to the routes. The default is 1.

Export OSPF Routes Metric

Use this field to specify that the Switch's OSPF routes are exported during RIP updates. You can also choose a metric value (1 through 15) to the routes or disable the export. The default is disabled.

Export Branch Office Static Routes Metric

If you have a branch office connection, use this field to export the static routes metric. This informs the remote branch office connection of the routes that are used for the connection and provides the metric value you assign to the routes. The default is 1 and the map value is 15.

VRRP

VRRP is configured on a per-interface basis and is only available on private Ethernet interfaces. VRRP must be configured on each system interface individually. Select Routing→Interfaces to access the Routing Interfaces screen. From this screen, you can configure the switch routing protocols for each system interface.

To configure VRRP on the interface, click the Configure button next to the VRRP Protocol on the Routing Interfaces screen. The Configure VRRP screen appears.

Figure 63 Routing Interfaces→Configure VRRP

SYSTEM

SERVICES

ROUTING

QOS

PROFILES

SERVICES

ADMIN

STATUS

HELP

STATIC ROUTES

OSPF

RIP

INTERFACES

VRRP

ROUTE TABLE

ACCESS LIST

POLICY

STATUS

Routing Interfaces --> Configure VRRP

HELPLOGOFF

Edit : 10.0.16.146

Configured State

Disabled

Master Status

Serve as Master	VRID	Operational State
Disabled	0	

OK

Cancel

Current Backed up Addresses

Backed Up Address	VRID	Configured State	Operational State	Priority	Actions
-------------------	------	------------------	-------------------	----------	---------

New Backed up Address

Backed Up Address

(none defined)

Priority

100

Add

Close

Configured State

The Configured State drop-down list box shows the current state, enabled or disabled. Select the desired state from these options.

Master Status

This section of the Configure VRRP screen is where you configure this interface to serve as a master for its own address.

Serve as Master

This drop-down list box lets you enable or disable this interface as a VRRP master of its own address. Enabled means that it serves as master. In order to enable mastership, there needs to be an entry in the Routing→VRRP screen with an IP address that matches this interface's address. The owner of the interface should have the option Serve as Master enabled.

Click OK after making a selection to effect the change.

VRID

The VRID column shows which VRID is used.

Operational State

Operational state shows the current running operational state, either Master or Backup.

Current Backed Up Addresses

The Current Backed Up Addresses section shows information about the currently configured backups. It shows what IP addresses this interface is backing up, the VRID it is using, its configured state (Enabled or Disabled), the current operational state and its priority. Multiple backups for the same address should have different priorities.

Edit

The Edit button allows you to enable or disable the backup address and to change its priority.

New Backed Up Address

New Backed Up Address allows new backups to be added. The pull down list here shows all the IP addresses set in the Routing→VRRP screen minus this interface's address and any other address that is already being backed up.

Backed Up Address

This list shows all the IP addresses set in the Routing→VRRP screen, minus this interface's address and any other address that is already being backed up.

Priority

The priority field specifies the sending VRRP router's priority for the virtual router. Higher values equal higher priority.

VRRP routers that are backing up a virtual router must use Priority Values between 1-254 (decimal). The default Priority Value is 100 (decimal).

If there are multiple backups, the Priorities should be scattered widely. For example, use Priority Values such as 50, 100, and 150, instead of 100, 101, and 102.

Add

Click Add to add the address selected from the New Backed Up Address list box to the list of Current Backed Up Addresses.

VRRP

Virtual Router Redundancy Protocol (VRRP) is one method you can use to configure the switch to maintain a state of High Availability. VRRP is a standard protocol that handles private interface failures. VRRP targets hosts that are configured with static next-hop routing addresses or default gateways. It provides a means of re-routing traffic in the event of a system/interface failure.

VRRP Configuration

VRRP is managed as two separate parts. The first part handles those configuration parameters that must be the same between all switches that make up a VR (Virtual Route).

Use of an external LDAP server makes it easier to configure VRRP because it provides a common location in which information about each switch in the system can be maintained. Use of an external LDAP server enables each switch to see the settings of other switches on the system. Configuration of VRRP requires that VRIDs (Virtual Router IDs) are agreed to by all participating switches.

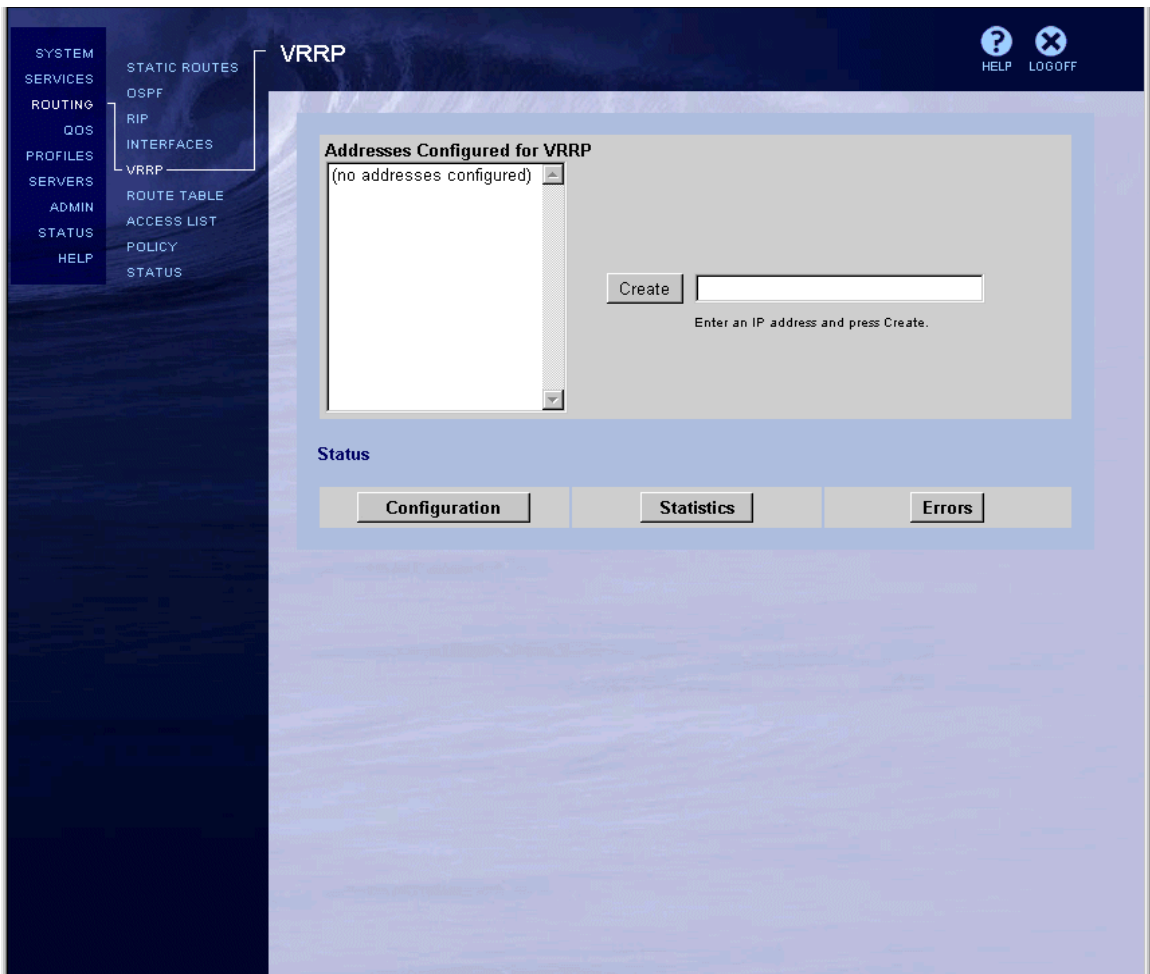
An external LDAP server is not a requirement. If the internal LDAP server is being used then the various switches must have these parameters configured the same and the responsibility for doing so lies with the administrator.

The second part of VRRP configuration is the information that is specific to a switch. This is information that is related to an interface and the role that the interface plays in VRRP (master or backup). This information is kept in the normal configuration file that is stored on the switch.

VRRP Screen

The Routing→VRRP screen lets you configure addresses for the Virtual Router Redundancy Protocol (VRRP). It also provides access to configuration information, statistics, and error information for VRRP addresses.

Figure 64 VRRP screen



Addresses Configured for VRRP

This list box shows all IP addresses that have been configured for use with VRRP.



Note: Only 1 IP address per Virtual Router (VR) is allowed.

IPSec AH (Authentication Handling) is not supported as an authentication option.

Edit

Select the VR that you want to modify from the Addresses Configured for VRRP list and click Edit. The Create/Edit VRRP IP Address screen appears. The Edit VRRP IP Address screen is the same as the Create VRRP IP Address screen.

Delete

Select the VR that you want to delete from the Addresses Configured for VRRP list and click Delete.

Create

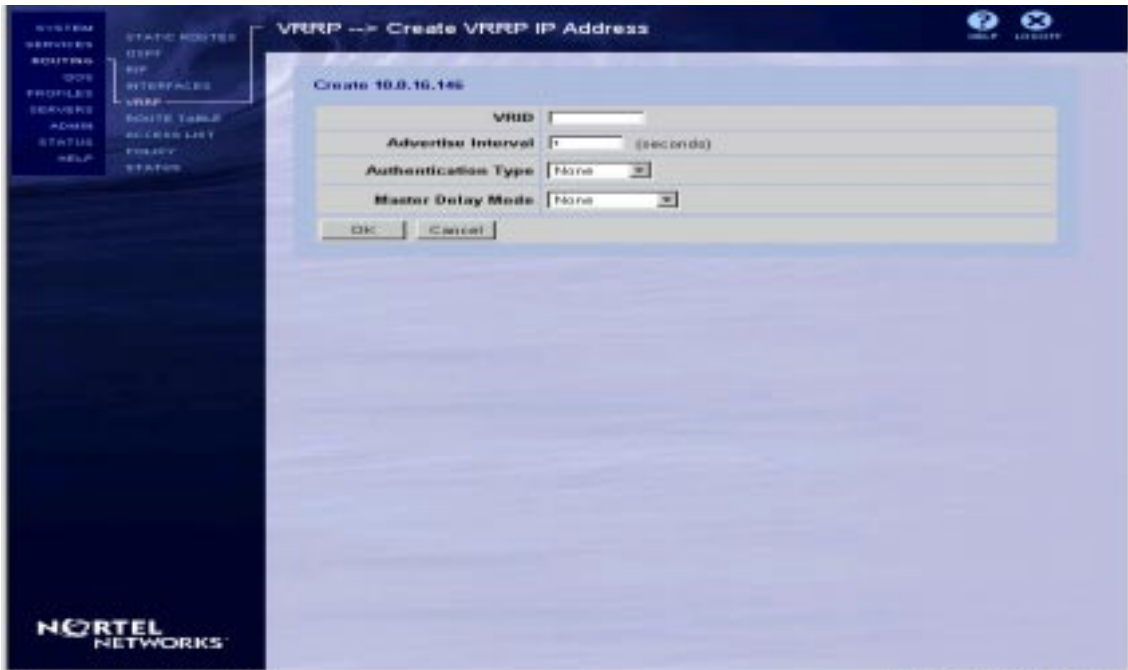
To create a new Virtual Router, enter the IP address in the IP Address field and click Create. The IP Address must match an Interface Address, as shown in the Routing→Interfaces screen, when configuring the VR as a Master.

The VRRP→Create/Edit VRRP IP Address screen appears when you click Create. You use this screen to configure the parameters for the VR you are creating.

Create/Edit VRRP IP Address Screen

The VRRP→Create/Edit VRRP IP Address screen appears when you click Create or Edit. You use this screen to configure the parameters for the VR you are creating or editing.

Changes to these parameters take effect only when VRRP is started on an interface, not while it is running. To make any changes take effect, disable VRRP on the Interface and then enable it.

Figure 65 VRRP→Create/Edit VRRP IP Address

VRID

Enter a decimal value in the range 1-255 for the Virtual Router ID (VRID). The VRID must be unique to the LAN segment running VRRP.

Advertise Interval

Enter the interval, in the range 1-255 seconds, at which the VR will advertise its virtual MAC Address. The default is 1 second.



Note: VRRP advertisements are sent to the 224.0.0.18 multicast IP address.

Authentication Type

Select the Authentication Type for this VR, either None or Simple.

Selection of None means that VRRP protocol exchanges are not authenticated. Nortel Networks recommends this type of authentication for environments with minimal security risk and little chance for configuration errors.

Selection of the Simple authentication type means that VRRP protocol exchanges are authenticated by a simple text password. Nortel Networks recommends this type of authentication when there is minimal risk of nodes on a LAN actively disrupting VRRP operation.

Authentication Data

Enter up to 8 characters of text. Any VRRP packet received with an authentication string that does not match the locally configured authentication string is discarded.

Confirm Authentication Data

Enter the same 8-character text password in this field as entered in the Authentication Data field to confirm it.

Master Delay Mode

Master Delay Mode controls when a switch takes mastership of an IP address it owns. Normally, this occurs when the interface becomes enabled. With Master Delay Mode it is possible to delay when this happens. Reasons for using Master Delay Mode include: you might want to wait to ensure that the switch is stable before having it start processing data; or you might want to wait until a slow period of the day to move traffic back.

Master Delay Mode controls when a switch takes back its IP addresses. It has no effect on the underlying VRRP protocol. A switch with Master Delay Mode enabled interoperates with another Switch that does not support Master Delay Mode.

Master Delay Mode is optional. The default for a VR is that Master Delay Mode is disabled (None).

Master Delay mode operates in one of two possible ways: Delay or Time of Day.



Note: The Safe Mode feature has the following interaction with Master Delay Mode: When safe mode is enabled, a boot after an unclean failure starts the safe mode image, instead of the normal boot image. If the safe mode image is configured with VRRP then Master Delay Mode works. However, safe mode automatically boots the normal image after some delay. This boot looks as though it was after a clean shutdown and Master Delay Mode is not invoked.

Delay

The Delay mode causes the switch to wait a given amount of time, after a system boot or after the circuit comes up, before the switch asserts its mastership. When you select Delay, the Master Delay Delta field appears on the screen. Enter the Delay time in this field in the form *hh:mm:ss*.

Time of Day

Time of Day mode allows a specified period, or window, of time to be set. Time of Day specifies the start of a window of time (in 24-hour format), and Delay specifies the size of that window of time. If the switch is booted or the circuit comes up within that window, then the switch immediately assumes mastership as though Master Delay mode was not in effect. If the switch is booted or the circuit comes up outside the specified window of time, then the switch waits until the beginning of the window before assuming mastership.

When using an external LDAP database, the following read-only fields appear, providing additional information about external Switches.

Master CES

This field displays the serial number of the switch configured to be Master of this address.

Backup CES

This field displays the serial number, name and priority of other switches configured as backups for this address.

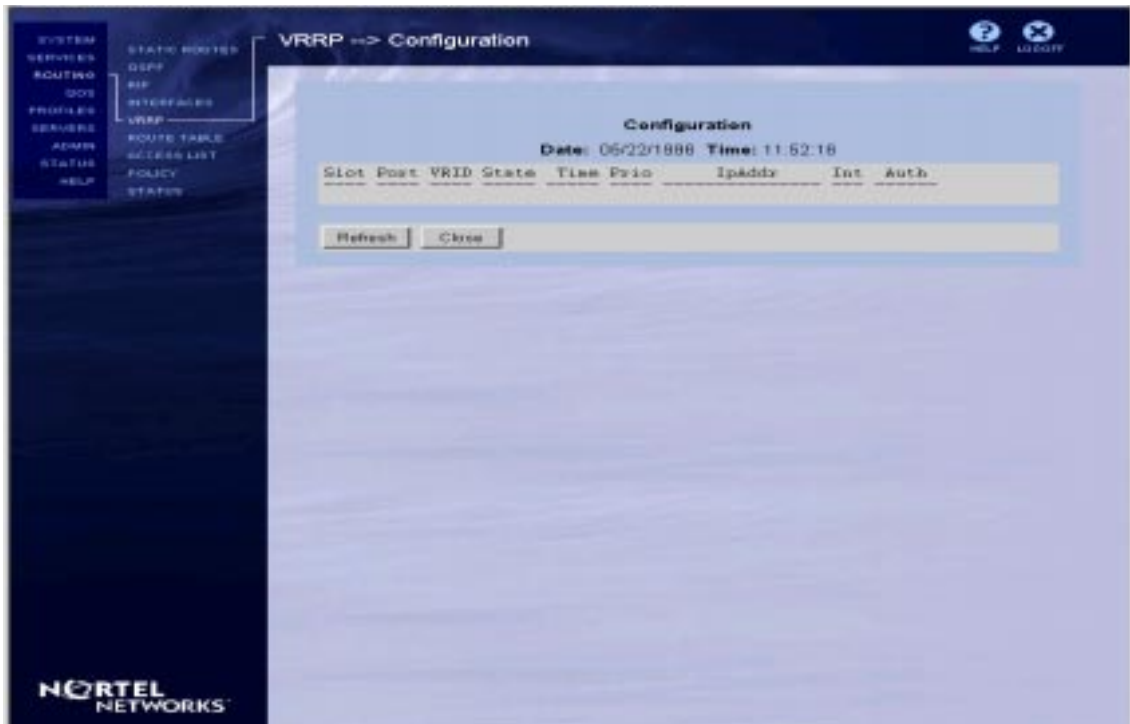
Status

The Status section of the VRRP screen provides buttons for accessing information about VRs. This includes configuration, statistics, and error information.

Configuration

You can view configuration information for a VR using the Configuration button. Select from the list of Addresses Configured for VRRP and then click Configuration.

Figure 66 VRRP→Configuration



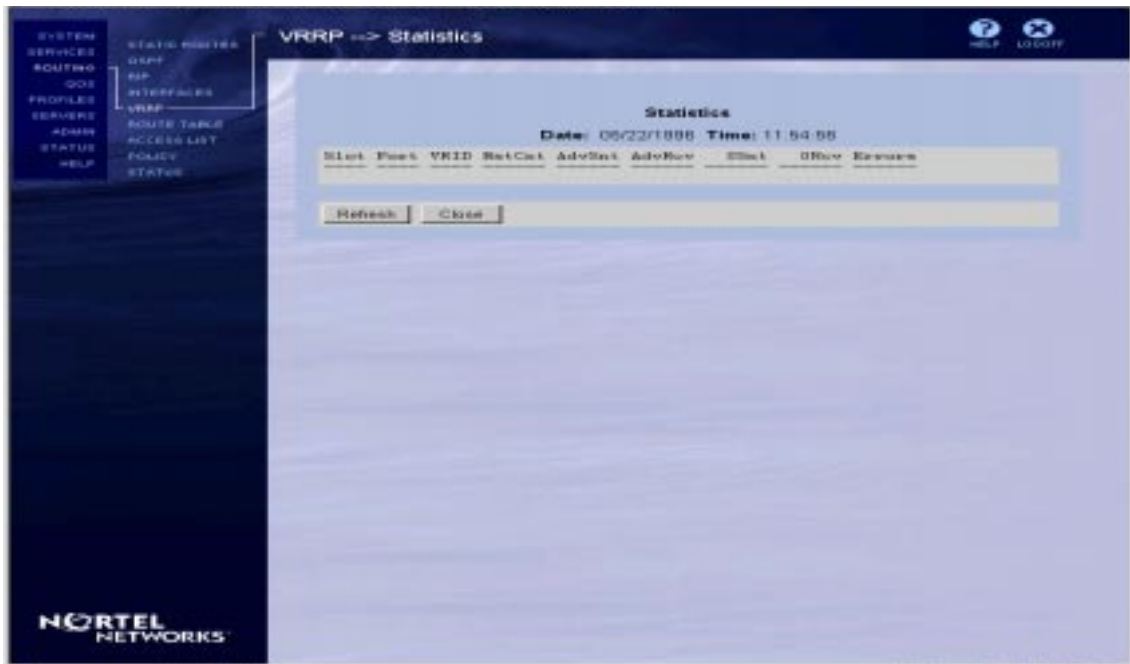
The following table describes the fields on the VRRP configuration screen.

Table 16 VRRP configuration information

Column	Description
Slot	Slot number associated with the interface on which this VR is configured.
Port	Port number associated with the interface on which this VR is configured.
VRID	Virtual Router ID number.
State	Operational state for this configuration, either M (Master) or B (Backup).
Time	(Hours:minutes) in this particular state
Prio	Shows the Priority level of this VR configuration
IpAddr	IP Address of this VR configuration.
Int	Advertisement interval
Prmt	Preempt Mode setting, either True or False.
Auth	Authentication type for this configuration, either None or Simple

To view statistical information about a VR, select from the list of Addresses Configured for VRRP and then click Statistics.

Figure 67 VRRP→Statistics



The following table describes the fields on the VRRP Statistics screen.

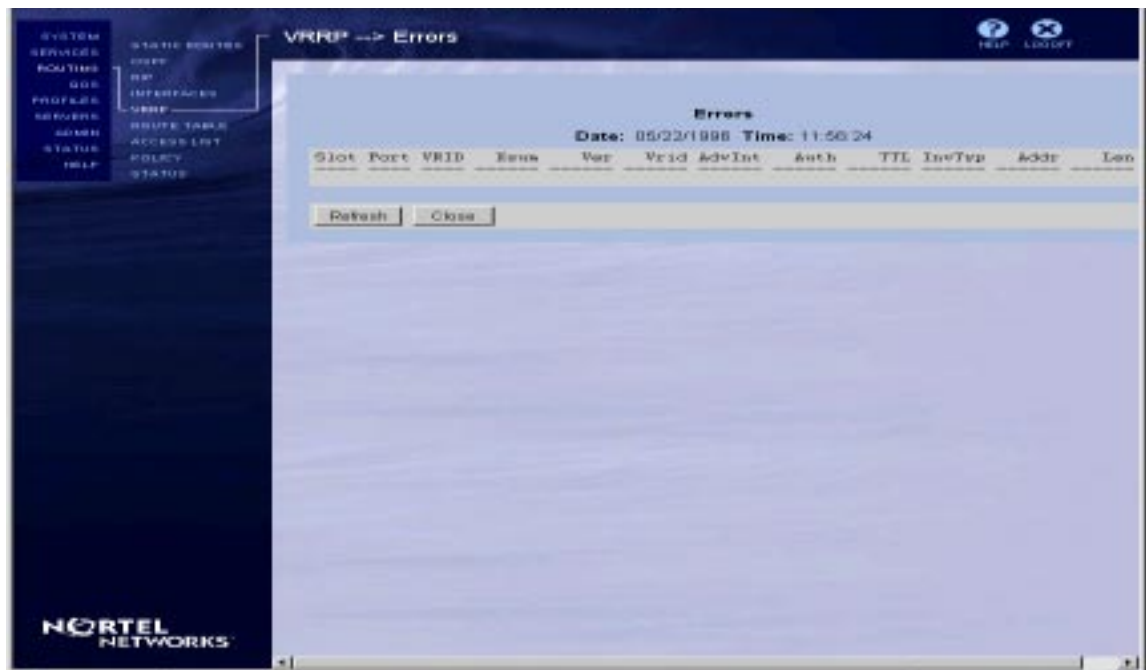
Table 17 VRRP Statistics

Column	Description
Slot	Slot number associated with the interface on which this VR is configured
Port	Port number associated with the interface on which this VR is configured.
VRID	Virtual Router ID number
MstCnt	Number of times this switch became master of this address.
AdvSnt	Number of advertisements broadcast by this VR.
AdvRcv	Number of advertisements received by this VR.
OSnt	Number of advertisements with a priority of 0 that were sent. Priority 0 advertisements are sent when VRRP is shutdown on an interface. They allow a backup to take over immediately.
ORcv	Number of advertisements received with a priority of 0.
Errors	Shows the number of errors that have occurred

Errors

To view error information about a VR, select from the list of Addresses Configured for VRRP and then click Errors.

Figure 68 VRRP→Errors



The following table describes fields on the VRRP Errors screen.

Table 18 VRRP Errors

Column	Description
Slot	Slot number associated with the interface on which this VR is configured.
Port	Port number associated with the interface on which this VR is configured.
VRID	Virtual Router ID number.
Xsum	Number of packets received that had bad Checksums
Ver	Number of packets received that specified an unsupported version of VRRP

Table 18 VRRP Errors

Column	Description
Vrid	Number of packets received that indicate a VRID that is not configured on this interface.
AdvInt	Number of packets received with incorrect Advertisement Intervals
Auth	Number of packets that failed Authentication
TTL	Number of packets received with an invalid TTL value in the IP header.
InvTyp	Number of packets received with invalid VRRP packet types.
Addr	Number of packets received that specified the incorrect IP address for this VR
Len	Number of packets received that had an incorrect length

Route Table

The route table contains routes submitted by the routing protocols and the static routes. Dynamic protocols such as OSPF and RIP submit the best route in their view for a specific destination. The switch stores all of the static routes and default routes in the route table. The route table manager chooses the best route based on the following order of protocol priority: direct route, static route, OSPF route, RIP route, default route. With this and the protocol cost, the route table manager selects the best route and forwards into the forwarding table. This screen provides information about the current routing table, and it allows you to view the routes using filter search criteria and save the information in a file.

Figure 69 Route table filter criteria screen

The screenshot shows the 'Route Table' configuration screen. On the left is a sidebar menu with the following items: SYSTEM, SERVICES, ROUTING, QOS, PROFILES, SERVICES, ADMIN, STATUS, and HELP. Under 'ROUTING', there is a sub-menu with: STATIC ROUTES, OSPF, RIP, INTERFACE, UNRP, ROUTE TABLE, ACCESS LIST, POLICY, and STATUS. The 'ROUTE TABLE' item is selected. The main content area has a title bar with a question mark and a close button. Below the title bar, the 'Route Table' section contains three search criteria: 'Search for' (set to 'All'), 'Interface' (set to 'All'), and 'Protocol' (set to 'All'). Each criterion has a dropdown arrow. Below these is a 'Search' button. The 'Save Route Table' section includes a 'Directory /Idell/system' label, a 'Filename' input field, and a 'Save' button. At the bottom, there are two buttons: 'IP Forward Table' and 'Route Table'.



Note: To obtain the total number of routes that are in the routing table, go to the Routing→Status screen and click on Route Table Stats.

Search For

Select the All, Host, or Network option. If you select Host, you can select whether the interface is All or choose the address from the Interface drop-down list. From the Protocol drop-down list, select All or the protocol (OSPF, RIP, Static, or Direct). You must enter the IP address in the edit box.

If the destination is Network, you can select whether the interface is All or choose the address from the Interface drop-down list. From the Protocol drop-down list, select All or the protocol (OSPF, RIP, Static, or Direct). You must enter the IP address and the Network Mask in the edit boxes. You can choose the Exact or Best Match from the Search Type drop-down list.

Interface

Select All or the current switch interface.

Protocol

Select All or OSPF, RIP, Static, or Direct.

Save Route Table

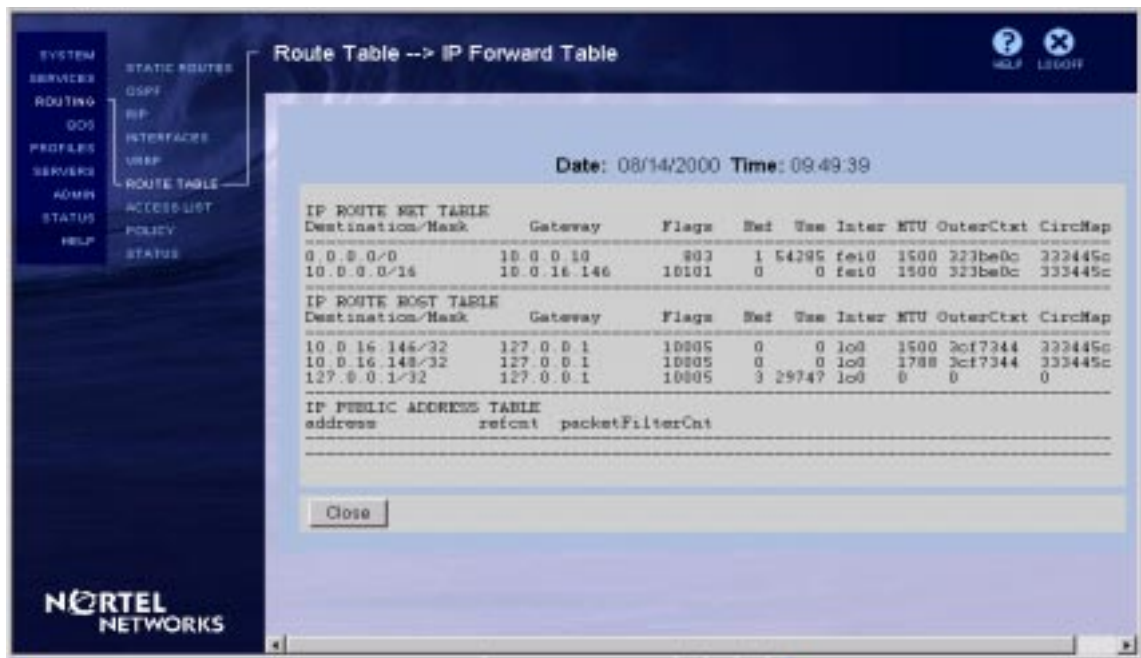
You can save the route table as a text file in the directory `ide0/system/xxx/`, where `xxx` is the name of the file that you specify.

Status

IP Forward Table

The IP forwarding table displays the following information for the IP Route Network Table, the IP Route Host Table, and the IP Public Address Table.

Figure 70 Route Table→IP Forward Table Screen



The following table describes fields on the IP Forward Table screen.

Table 19 IP Forward Table Screen

Column	Description
Destination/Mast	Network address and mask
Gateway	IP address of next hop gateway
Flags	Internal use flags
Refcnt	Reference count
Use	How many time used
Interface	Interface identifier
MTU	Size of packet
OuterCtxt	(For internal use only)
CircMap	(For internal use only)
RtEntryP	(For internal use only)

Route Table

The full internal routing table displays all routing information.

Figure 71 Route Table→Route Table

Route Table --> Route Table

HELP LOGOFF

Route Table

Date: 06/07/2000 Time: 15:48:48

Show the Full Route Table

Seq	Proto	Ip Address/NetMask	Weight	NextHop	NextHopInterface	CI
5	Static	0.0.0.0/0	a	10.0.0.10	10.0.16.148	1
3	Direct	10.0.0.0/16	0	10.0.16.148	10.0.16.148	1
2	Direct	10.0.16.148/32	0	127.0.0.1	127.0.0.1	1
Total Host Routes = 0						
Total Network Routes = 3						

Show the Best Route Table

Seq	Proto	Ip Address/NetMask	Weight	NextHop	NextHopInterface	CI
2	Direct	10.0.16.148/32	0	127.0.0.1	127.0.0.1	1
3	Direct	10.0.0.0/16	0	10.0.16.148	10.0.16.148	1
5	Static	0.0.0.0/0	a	10.0.0.10	10.0.16.148	1
5 RIP BookMark (OSPF, Static, Direct)						
5 FEM BookMark (RIP, OSPF, BGP, Static, Direct, Mgmt, FEM)						
Total Reachable Routes = 3						
Total Deleting Routes = 0						
Total BookMarks = 2						

Show the Next Hop Table

Next Hop Address	Linked	Primary Route	NextHopInterface	CId	Ref	isRe
10.0.0.10	To Direct	10.0.16.148	10.0.16.148	1	1	Ye
10.0.16.148	To Direct	10.0.16.148	10.0.16.148	1	1	Ye
127.0.0.1	To Self	10.0.16.148	127.0.0.1	1	1	Ye
3 Next Hop Entries						

Close

NORTEL NETWORKS

The following table describes fields on the IP Routing Table screen.

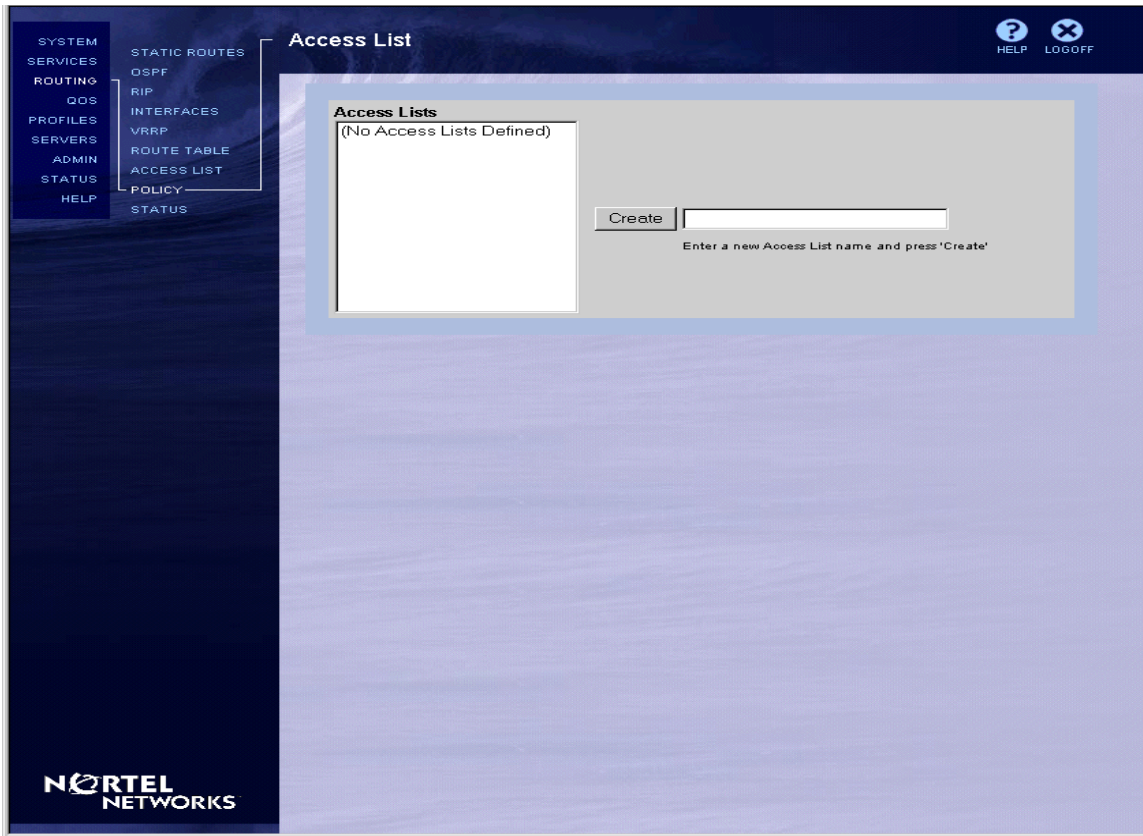
Table 20 IP Routing Table

Column	Description
Seq	Sequence number that shows the best route
Proto	Protocol
IP Address/Netmask	IP Address/NetMask
Weight	A combination of cost and priority for the best route
NextHop	IP address of the next hop
NextHopInterface	IP address of the next hop interface
CId	Circuit ID

Access List

Routing policies are based on a set of rules that result in actions. However, you can have access lists that are part of any policy. An access list contains these rules and actions, which allows you to use the same set of rules for different protocols. These rules are tested in order until the first match is found, which then causes the action to occur. Routing policies have an implicit deny all rule, which means that if no rule matches then access is denied; no traffic is transmitted or received unless it is specifically permitted.

The Access Lists screen displays all previously created lists. You can edit or delete a selected list name or create a new one.

Figure 72 Access List

Create

Type in the name of the access list in the edit box and click on the Create button to create a new access list. You can use any name or number that you choose to a maximum length of 64 characters.

Figure 73 Access List→Create

Access List --> Create

Current Rules for Access List : test

Rule	Action	Subnet	Mask	Mask Type
1: Permit All 0.0.0.0 0.0.0.0 Range	Permit			Exact

New Rule

Action: (for Permit All and Deny All ignore Subnet, Mask and Mask Type)

Subnet:

Mask:

Mask Type:

Add Close

Current Rules for Access List: xxx

Edit

Click on the Edit button to change the existing rule for the selected policy. The current information appears for each policy. You can use either an exact network address or a range of network addresses.

Figure 74 Access List→Edit

Access List --> Edit

Current Rules for Access List : xyz

(No rules defined in Access List)

New Rule

Action: (for Permit All and Deny All ignore Subnet, Mask and Mask Type)

Subnet:

Mask:

Mask Type:

NORTEL NETWORKS

Delete

Click on the Delete button to delete the selected rule.

Move selected rule to position

Entering a number in the edit box allows you to specify the position of an existing rule. For example, if you select the third rule and enter 2 in the edit box, this moves the third rule to the second position. Selecting the order of the rules is important because the first match causes the action to occur. If there are no matches, then all traffic is denied. Therefore, you should build your filter rules by first permitting the services that you want to allow. You also might want to add a Deny rule early in the rules sequence so that an unwanted packet is dropped before processing all of the rules.

New Rule

Click on the Create button to add a policy to the policy list. This displays the Access List→Edit screen.

Action

Options are Permit, Deny, Permit All or Deny All. Permit or Deny is the action applied to a route update when the subnet and mask matches the route update. If you choose Permit All or Deny All, you cannot enter anything in the Subnet, Mask or Mask Type fields.

Subnet

IP address of the subnet for which you want to create a rule. Subnet is the number of the network. The subnet should be specified using a 32-bit quantity in four-part, dotted-decimal format.

Mask

Subnet mask of the subnet for which you want to create a rule. Mask is the network mask to be applied to subnet. The network mask is a 32-bit quantity in four-part, dotted-decimal format. Place zeroes in the bit positions you want to ignore.

Mask Type

Specify Exact or Range.

Policy

Policies are used to control reachability by allowing or restricting routing information. RPS controls the flow of routing data to and from the routing table. Routing policies are based on a set of rules that result in actions. Routing policies have an implicit deny all rule, which means that if no rule matches access is denied.

An access list that contains this set of rules and conditions allows you to use the same set of rules for different protocols. Redistribution allows route updates to be redistributed from one routing domain into another routing domain. It helps connect networks of different protocols by allowing specified redistributed routes to know about networks that are not normally advertised.

The Policy screen allows you to set up the routing policies.

Figure 75 Routing Policy Service

Policy

Route Policy Service

Enabled ☒

Redistribution Table

Protocol	Route Source		
OSPF	☐ Static	☐ Direct	☐ RIP
RIP	☐ Static	☐ Direct	☐ OSPF

OK Cancel

Policy List

Protocol	Access Name/Number	Interface	Type	Action
Add				

NORTEL NETWORKS

Route Policy Service

Check the Enabled box to enable RPS. The default setting is enabled.

Redistribution Table

Protocol

The name of the protocol, either OSPF or RIP.

Route Source

The source of the route for each protocol, either Static, Direct, or RIP.

Policy List

Access Name/Number

This is a way to identify the policy. This can be any name or number that you choose. A numbered access list can use numbers between 1 and 99. A named access list can be any alphanumeric name that begins with a letter of the alphabet. You need to create an Access list before creating policy entries. To create the list, click on the New Access List link. This displays the Access Lists screen with all named items listed. You can edit or delete a selected list name or create a new one by typing the name in the edit box.

Protocol

The name of the protocol, either OSPF or RIP.

Interface

IP address of the physical interface where you want to apply the policy. Use 0.0.0.0 if you want to apply the policy for all interfaces. Use the tunnel endpoint IP address for tunnels.

Policy Type

Accept or announce policy. You can have only one Accept or Announce policy for each protocol per interface.

Action

Edit

Click on the Edit button to edit the selected policy.

Delete

Click on the Delete button to delete the selected policy.

Add

Click on the Add button to display the Policy→Add screen. Enter the Protocol, Access Name/Number, Interface, and Policy Type.

Figure 76 Policy→Add

The screenshot displays the Nortel Networks configuration interface. On the left is a dark blue sidebar with a menu containing: SYSTEM, SERVICES, ROUTING, QOS, PROFILES, SERVERS, ADMIN, STATUS, HELP, and POLICY (which is highlighted). To the right of the sidebar, under the 'POLICY' section, are sub-items: STATIC ROUTES, OSPF, RIP, INTERFACES, VRRP, ROUTE TABLE, ACCESS LIST, and STATUS. The main window is titled 'Policy --> Add' and includes 'HELP' and 'LOGOFF' buttons in the top right. It contains two sections: 'Policy List' and 'New Policy'. The 'Policy List' section has a table with the following data:

Protocol	Access Name/Number	Interface	Type
RIP	deny_9.9.9.9_only	0.0.0.0	ACCEPT

The 'New Policy' section contains the following fields:

- Access Name/Number:** A dropdown menu showing 'deny_10.254.52.0_only' and a link to 'New Access List'.
- Protocol:** A dropdown menu showing 'OSPF'.
- Interface:** A dropdown menu showing '10.254.1.85 (Physical Interface)'.
- Type:** A dropdown menu showing 'Announce'.

At the bottom of the 'New Policy' section are three buttons: 'OK', 'Apply', and 'Cancel'. The Nortel Networks logo is visible in the bottom left corner of the interface.

Client address redistribution

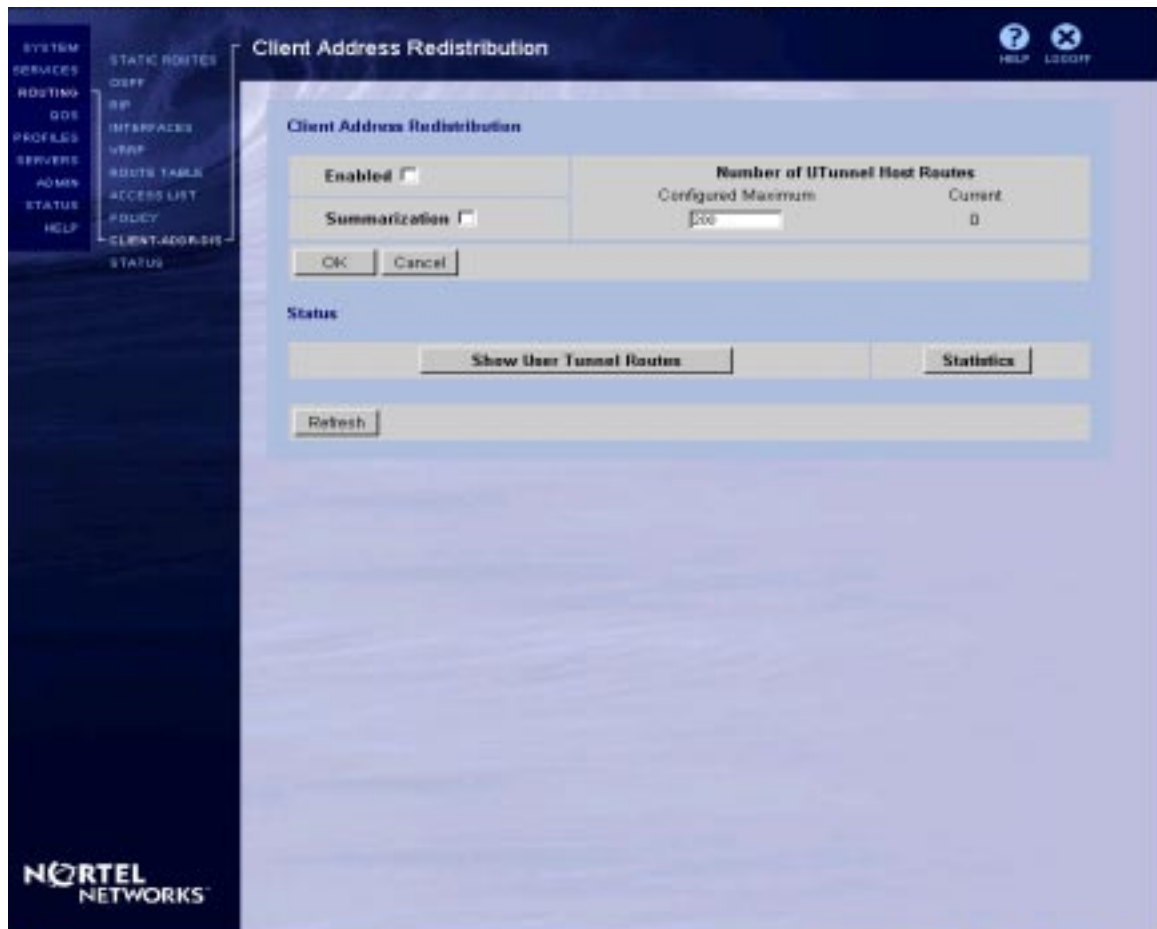
Client address redistribution allows the switch to advertise user tunnel host network routes if the private address does not belong to a locally attached switch network. It dynamically advertises one route for each connected client, which begins when the client logs in and ends when the client logs out. This is the default.

When client address redistribution is active, the switch creates and advertises a user tunnel host route whenever a client tunnel is created using an inner address that does not belong to a locally attached network. When the tunnel is disconnected, the corresponding host route is deleted..



Note: The maximum number of Utunnel routes cannot exceed the maximum number of client tunnels supported by the corresponding hardware platform. The default value is 200.

The Routing Table Manager handles a Utunnel route type that handles advertisement of these routes and they correspond to the Direct, Static, RIP, and OSPF types. Click Routing→Client-Addr-Dis to configure client address redistribution routes.

Figure 77 Client Address Redistribution

Client address redistribution

Enabled

Check the Enabled box to enable client address redistribution. If you enable client address redistribution, operations related to the Utunnel are effective. If you disable client address redistribution, the switch stops redistribution of all Utunnel routes. The routes remain in the route table, but are not advertised. Any existing user tunnels remain logged in, but may not be able to communicate with the private network and any new Utunnel routes are disallowed. The default is disabled.

Number of UTunnel Host Routes

Configured Maximum

This field allows you to limit the maximum number of user tunnel host route entries in the system. The default value is 200.

Current

This field displays the current number of user tunnel hosts logged in to the system.

Summarization

Check the Summarization box to enable summarization. If you disable summarization, the switch inserts a user tunnel host route for the client address into the route table. If you enable summarization, the switch identifies the subnet from the address pools where this address belongs and inserts a user tunnel network route for this subnet in the route table. The default is disabled.

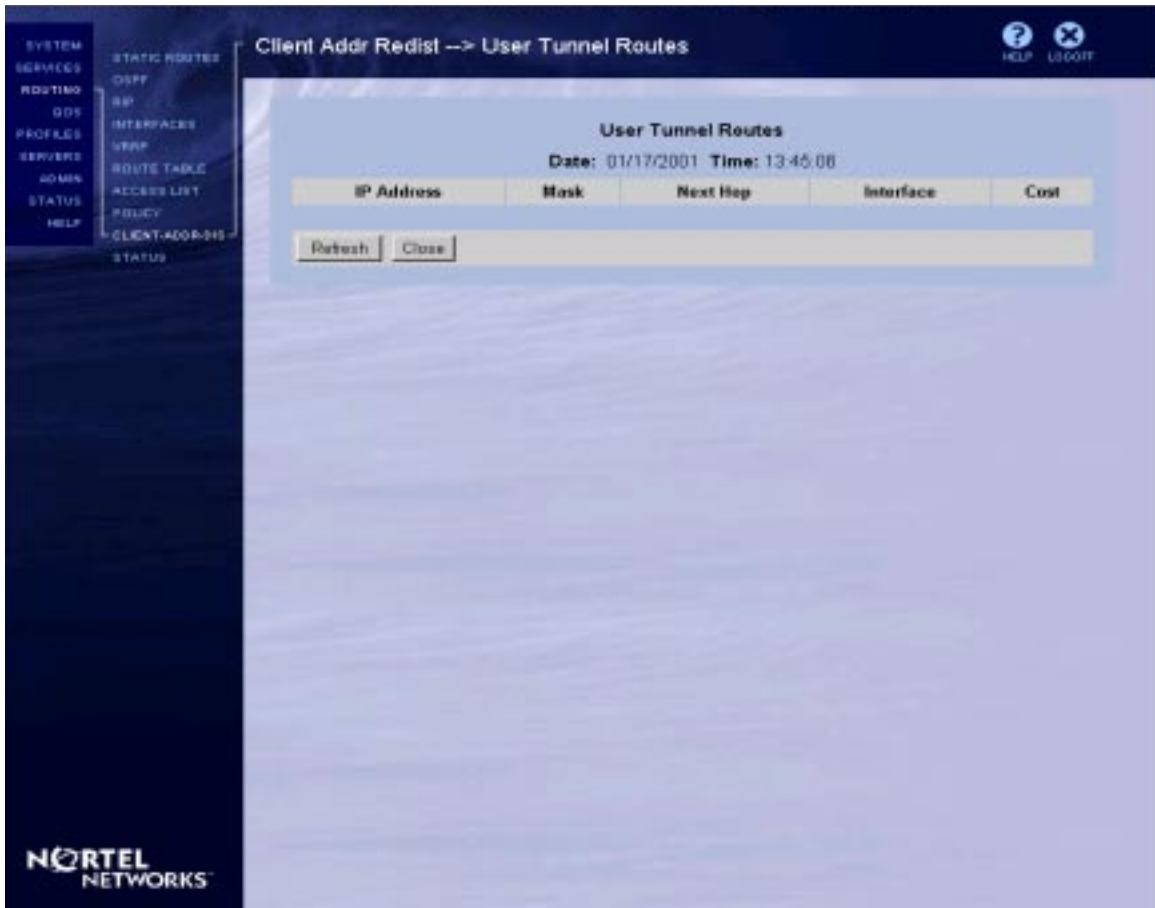


Note: The summarization option works only for address ranges that do not belong to the local subnet and that are allocated by the switch from an address pool.

Status

Show User Tunnel Routes

Click to display user tunnel routes.

Figure 78 Client Addr Redist→User Tunnel Routes

Statistics

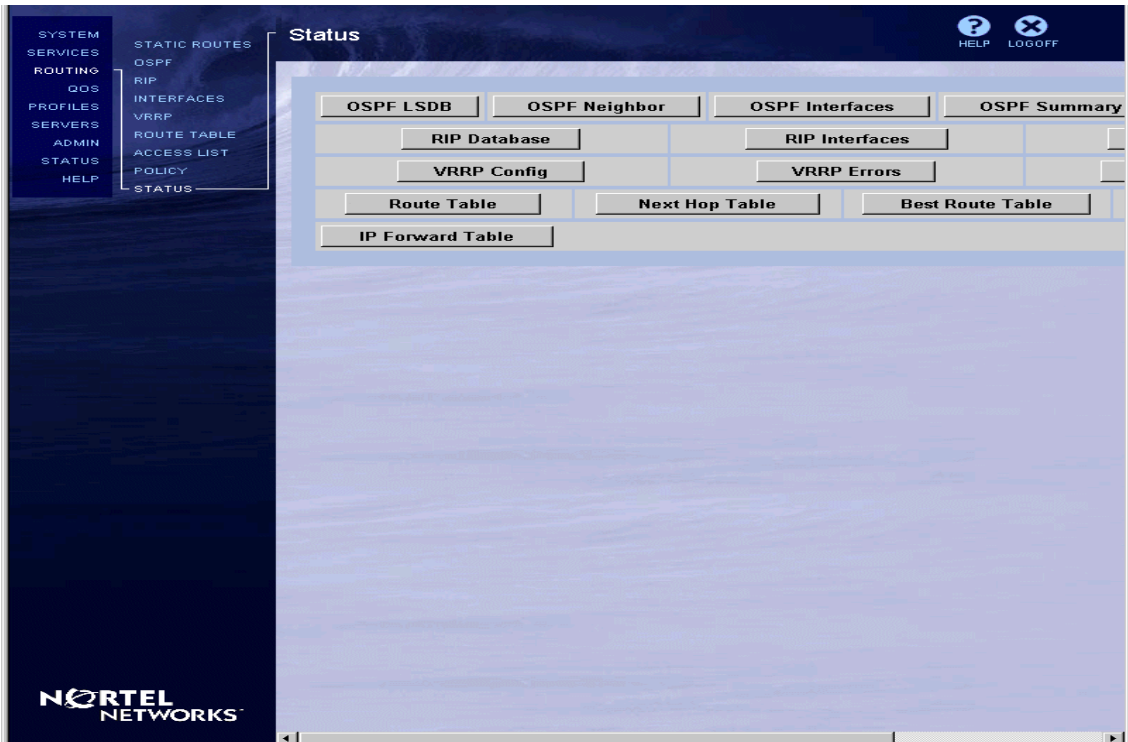
Click to display the configuration of client address redistribution, including whether it is globally enabled or disabled, the utunnel limit, current utunnel count, current utunnel redistribution configuration and summarization options. Table 21 describes these statistics.

Table 21 Client address redistribution statistics

Column	Description
IP address	IP address
Mask	IP network mask
Next Hop	Next hop address
Interface	IP interface address
Cost	Relative cost for the switch

Status

This screen provides access to information about the status of the OSPF, RIP and VRRP protocols. It also provides access to the Route Table and RTM Statistics. To view the information for each of these, click on the appropriate button.

Figure 79 Routing Status

OSPF LSDB

Lists the link state databases in all areas that are known to OSPF. For each area, it provides the link state type, ID, advertising router address, metric, ASE, forward address, age, and sequence number.

OSPF Neighbor

Shows the list of neighbors on all the interfaces running OSPF, including the IP interface address, router ID, neighbor IP address, state, and dead time priority.

OSPF Interfaces

Shows the list of interfaces that you configured for OSPF, including the IP address of the interface, the area to which the interface belongs, the type of interface, the state, cost and the designated router in the area to which the interface belongs.

OSPF Summary

Shows the overall summary of OSPF running on the switch. It specifies the router ID, global state (Up or Down), whether it is an area border router and whether it is an autonomous system border router.

OSPF Statistics

Shows system-wide OSPF statistics.

RIP Database

Shows the information contained in the RIP database.

RIP Interfaces

Shows the list of interfaces that you configured for RIP.

RIP Statistics

Shows system-wide RIP statistics.

VRRP Config

Shows VRRP configuration information.

VRRP Errors

Shows system-wide VRRP errors that have occurred.

VRRP Statistics

Shows system-wide VRRP statistics.

Route Table

Shows full routing for all routes, including next hops and best routes.

Next Hop Table

Shows the next hops for routes.

Best Route Table

Used by the forwarding table to determine the best route.

RTM Statistics

Shows statistics about routing table management that provides information about switch traffic.

IP Forward Table

Displays information for the IP route.

Chapter 4

QoS (Quality of Service)

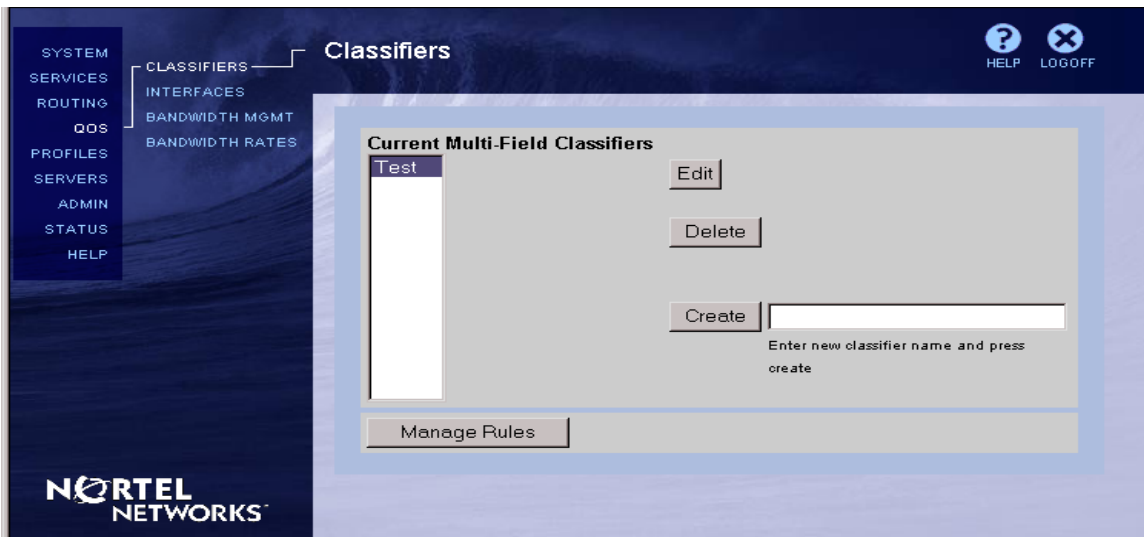
Quality of Service (QoS) is an area of functionality that provides settings for specifying the quality of network connections. QoS is implemented in the IP protocol by the DiffServ byte in the IP packet header.

The QoS menu includes screens that provide a convenient way to set and configure DiffServ (Differentiated Services) settings so you can ensure certain treatment, or Quality of Service, of data. QoS capabilities enable you to exert a specified level of control over data transmissions.

Classifiers

An MF Classifier can be defined for a user group (tunnel MF) or an interface (interface MF). The tunnel MF-Classifier is applied to tunnels brought up by users of that group. The interface MF-Classifier is applied to routing traffic going through that interface.

The MF Classifier applied to a group (tunnel MF) is configured within a group context through the Profiles→Groups screen. Interface classifiers are configured from the QoS→Classifiers screen.

Figure 80 QOS→Current Multi-Field (MF) Classifiers

Current Multi-Field (MF) Classifiers

The Current Multi-Field (MF) Classifiers list includes all existing MF Classifiers. You can edit and delete MF Classifiers by selecting from this list. These MF Classifiers can then be associated with user-groups, branch office connections, and physical interfaces.

Create

Enter a name for the new classifier in the field and click Create to create a new MF Classifier.

Delete

Select from the Current MF Classifiers and click Delete to remove the selected Classifier.

Edit

Select from the Current Multi-Field (MF) Classifiers and click Edit to edit the rules for that MF Classifier. The Edit Rule screen appears when you click Edit.

Rules in Classifier

The Rules in Classifier list shows all of the rules that are applied to the MF Classifier.

Available Rules

The Available Rules list shows all of the existing rules. You can select rules from this list to move them into the Rules in Classifier list and apply them to the MF Classifier.

<< (Add Rule)

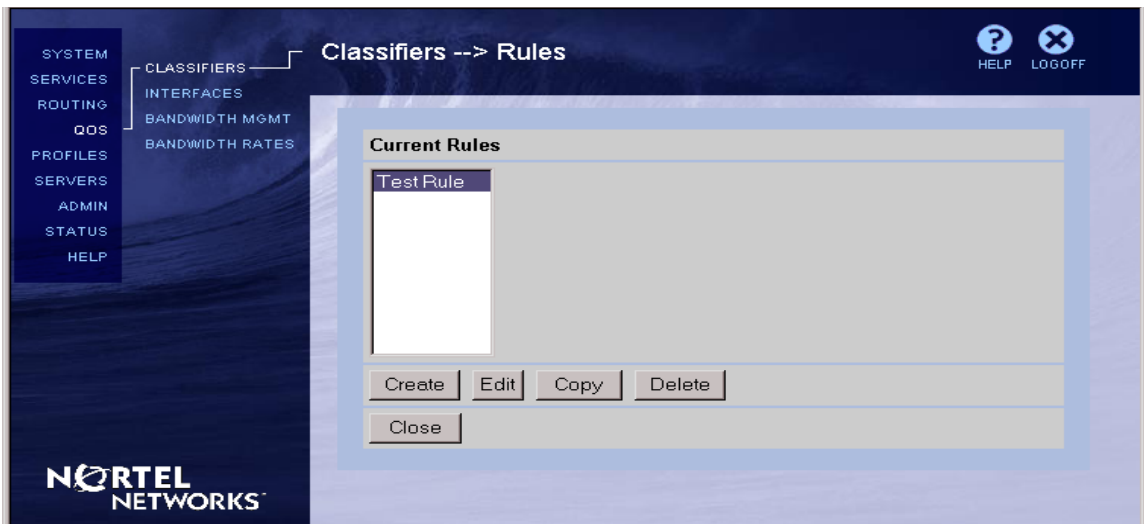
Click on a rule from the Available Rules list on the right of the screen, then click on the left arrow to add the rule. This adds the selected rule to the current rules list. The new rule is added after the rule currently selected in the Rules in Classifier list.

>> (Remove Rule)

Click on a rule, then click the right arrow to remove or delete it from the Rules in Classifier list.

Manage Rules

You use the Manage Rules button in the Edit Classifier screen to create and edit rules. When you click Manage Rules, the Current Rules screen appears. From this screen you can create, edit, copy and delete MF Classifier Rules.

Figure 81 QOS→Rules

Current Rules

The Current Rules list shows all existing rules. You can edit, copy or delete any of these existing rules.

Create

Click Create to create a new rule. The “Edit/Create Rules screen” appears when you click Create.

Edit

You can make changes to an existing rule by selecting it from the list of Current Rules and clicking the Edit button. The “Edit/Create Rules screen” appears when you click Edit.

Copy

You can use the Copy button to create a new rule that starts as a copy of an existing rule, which you can then edit. This is useful if you want to make minor changes to an existing rule. When you copy a rule, the “Edit/Create Rules screen” appears, populated with the settings of the rule you have copied.

Delete

To remove a rule, select it from the list of Current Rules and click Delete.

Edit/Create Rules screen

The Edit and Create Rules screens let you create and modify MF Classifier rules.

Figure 82 Classifiers→Rules→Edit/Create Rules

Classifiers --> Rules --> Edit Rule

CLASSIFIER Rule for: Test Rule

Source Address	any, 0.0.0.0, 255.255.255.255	Modify
Destination Address	any, 0.0.0.0, 255.255.255.255	
Protocol	ip	Modify
TCP/UDP Source Port	any, 0	Modify
TCP/UDP Destination Port	any, 0	
Current DSCP Value	any	Modify
DiffServ Marking	☒ Expedited Forwarding (EF) ☐ Assured Forwarding 1 (AF1) ☐ Assured Forwarding 2 (AF2) ☐ Assured Forwarding 3 (AF3) ☐ Assured Forwarding 4 (AF4)	

Note: DiffServ Code Point is always copied into tunnel headers.

OK Cancel

Classifier Rule for

When editing an existing rule, this field shows the name of the rule.

Source Address and Destination Address

Enter the Source and Destination addresses to limit the rule to acting on packets from and to these specified addresses.

Source and Destination are relative to the direction of the rule.

Modify Source & Destination Address

Click the Modify button to the right of the Source and Destination Address fields to edit either of these fields. The DiffServ→Rules Definition→Address screen appears.

Protocol

Click the drop-down list box to select the appropriate Protocol. To add, edit, or delete Protocols, click Modify. The default list follows:

- ICMP - Internet Control Message Protocol is a Network protocol layer. The PING utility generates ICMP packets. PING is often used to see if a system's network is available.
- IP - Internet Protocol is a Network layer protocol in the TCP/IP stack that offers a connectionless internetwork service. IP packets that are encapsulated within other packets create "IP over IP." Multicast IP packets (packets that have multicast destinations), carried between networks that support multicasting over intermediate networks that do not, are the most common implementation. Conferencing and other services that are offered through Multicast Backbone (MBONE) are examples.
- TCP - Transmission Control Protocol is a transport layer protocol in the TCP/IP protocol stack. This is a connection-oriented protocol that provides reliable full-duplex data transmission. Web browsers using HTTP and FTP are examples.
- UDP - User Datagram Protocol is a transport layer protocol in the UDP/IP protocol stack. UDP is a connectionless service that exchanges datagrams without acknowledgment or delivery guarantees, and therefore requires that error handling and retransmissions are handled by other protocols. DNS and WINS are examples.

Modify Protocol

Click the Modify button to the right of the Protocol field to edit the field.

TCP/UDP Source and Destination Ports

You can filter packets to or from the Source and Destination Ports. This would permit or deny any packets from being transferred by the Switch based on the Source and Destination Ports.

The Source or Destination is relative to the direction of the rule.

Modify TCP/UDP Source & Destination Ports

Click the Modify button to the right of the TCP/UDP Source and Destination Port fields to edit either of these fields.

Current DSCP Value

The DSCP Value & Mask assignments allow packets that are already marked to retain their settings or to be remarked based on their previous DSCP value.

Modify DSCP Value

Click the Modify button to the right of the Current DSCP Value field to create and edit the DSCP value and mask.

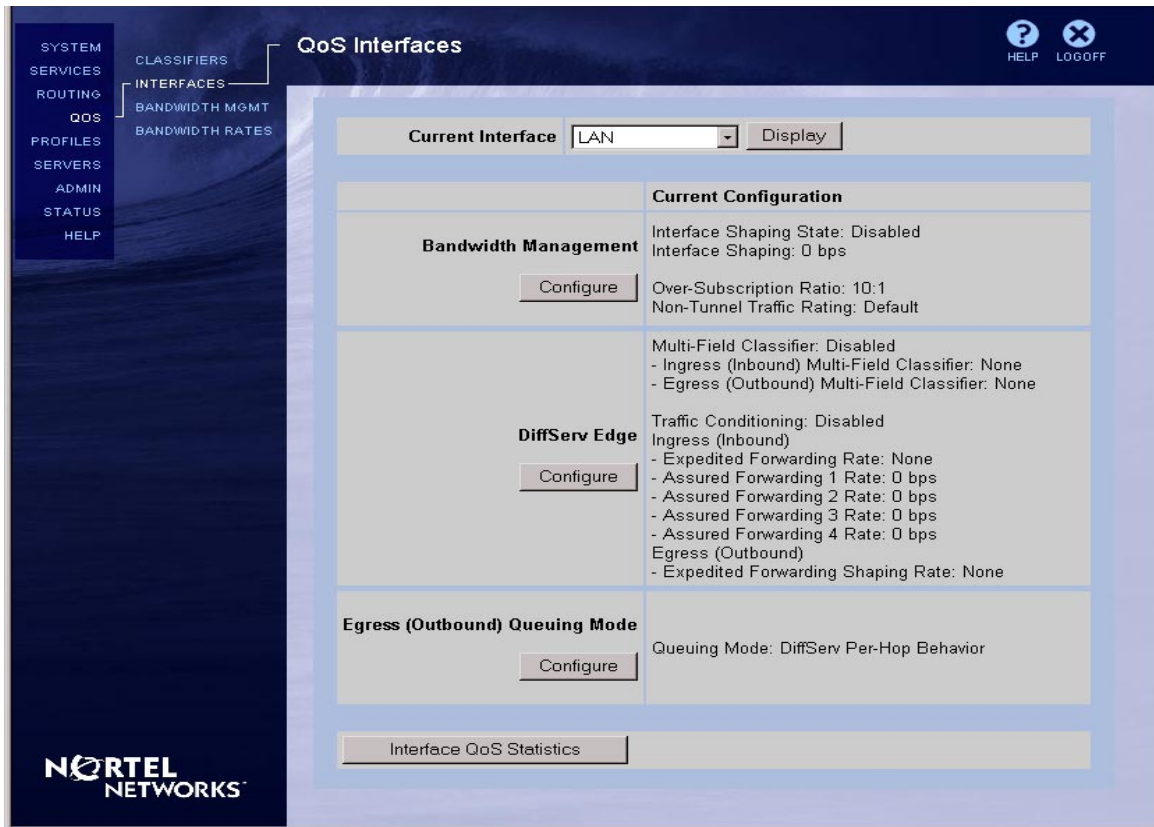
DiffServ Marking

Select the DSCP to be marked on the next meter, either EF (Expedited Forwarding) or an AF (Assured Forwarding) level, that this rule applies to data.

QoS Interfaces

The QoS Interfaces screen provides information about the QoS settings for each physical interface. This screen also enables you to view statistical information for each interface and to edit the QoS settings for each individual interface.

Figure 83 QoS Interfaces



Current Interface

For each physical interface, such as a LAN, the QoS Interfaces screen provides information about its current QoS settings. Select the physical interface from the list and click screen to see the QoS settings for a particular interface.

The Interface QoS Statistics button lets you view operational statistics for the Current Interface.

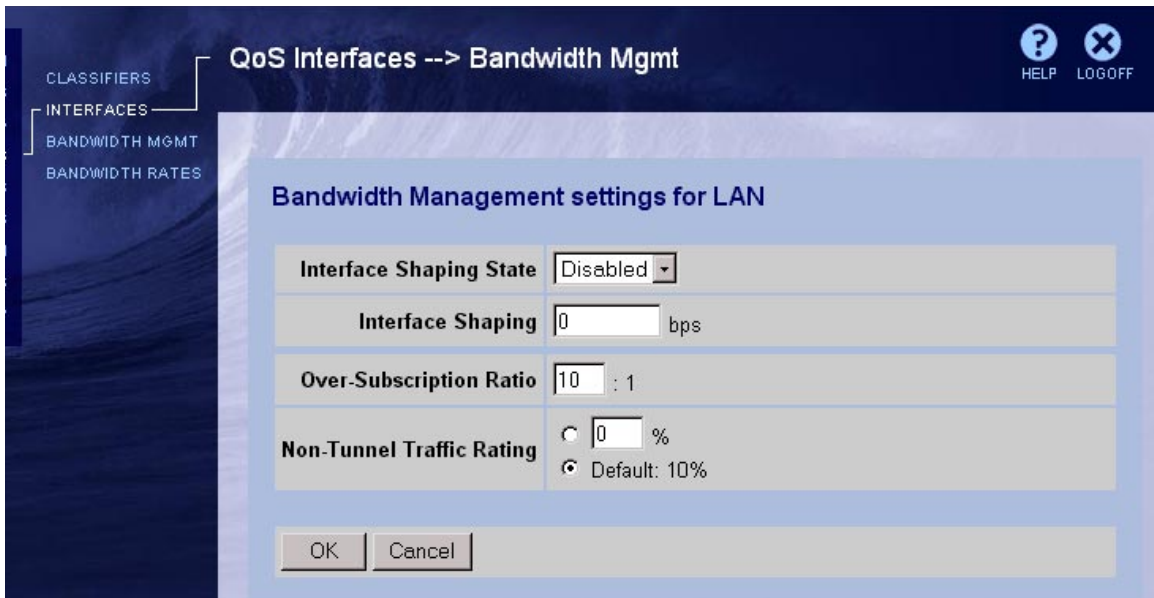
Bandwidth Management

The Bandwidth Management section of the QoS Interfaces screen shows the current Bandwidth Management settings for the selected physical interface. To change any of these settings, click the Configure button.

Configure

The Bandwidth Management screen appears when you click the Configure button. Use this screen to configure Bandwidth Management settings for the selected physical interface.

Figure 84 QoS Interfaces→Bandwidth Management→Configure



The screenshot displays the 'QoS Interfaces --> Bandwidth Mgmt' configuration window. On the left, a sidebar lists 'CLASSIFIERS', 'INTERFACES', 'BANDWIDTH MGMT', and 'BANDWIDTH RATES'. The main area is titled 'Bandwidth Management settings for LAN'. It contains four settings: 'Interface Shaping State' set to 'Disabled', 'Interface Shaping' set to '0 bps', 'Over-Subscription Ratio' set to '10 : 1', and 'Non-Tunnel Traffic Rating' with radio buttons for '0 %' (selected) and 'Default: 10%'. At the bottom are 'OK' and 'Cancel' buttons. In the top right corner, there are 'HELP' and 'LOGOFF' icons.

Setting	Value
Interface Shaping State	Disabled
Interface Shaping	0 bps
Over-Subscription Ratio	10 : 1
Non-Tunnel Traffic Rating	☒ 0 % ☐ Default: 10%

Interface Shaping State

Enable or disable Interface Shaping for this physical interface.

Interface Shaping

Enter a value, in bps, for Interface shaping. This value is used to shape (delay) the outgoing packet flow through an interface to better match the throughput of a downstream device. Non conforming traffic is delayed not dropped.

Over-Subscription Ratio

Configure for the interface how much of its bandwidth to over-subscribe. For example, for a value of 5 (5:1 Over-Subscription ratio) for a 1Mb T1 interface, the switch allows connections up to 5Mbit of total guaranteed bandwidth on the interface.

Non-Tunnel Traffic Rating

Enter a percentage of the total bandwidth to reserve for non-tunneled traffic on the selected interface. The default is 10 percent.

DiffServ Edge

The DiffServ Edge screen appears when you click the Configure button in the DiffServ section of the QoS Interfaces screen. Use this screen to configure DiffServ Edge settings for the selected physical interface.

Figure 85 QoS Interfaces→DiffServ→Configure

QoS Interfaces → DiffServ Edge

Multi-Field Classifier

Multi-Field Classifier State:

Ingress (Inbound)	Egress (Outbound)
Multi-Field Classifier: (No MF Classifiers Defined)	Multi-Field Classifier: (No MF Classifiers Defined)

Traffic Conditioning

Traffic Conditioning State:

Ingress (Inbound)	Egress (Outbound)
Expedited Forwarding Rate: ☐ 0 bps ☒ None	Expedited Forwarding Shaping Rate: ☐ 0 bps ☒ None
Assured Forwarding 1 Rate: 0 bps	Multi-Level Random Early Detection (MRED)
Assured Forwarding 2 Rate: 0 bps	
Assured Forwarding 3 Rate: 0 bps	
Assured Forwarding 4 Rate: 0 bps	

OK Cancel

Multi-Field Classifier

Multi-Field Classifier State

Use the drop-down list box to enable or disable the application of MF Classifiers on this interface.

Ingress (Inbound) MF Classifiers

Select from the list of existing MF Classifiers the MF Classifier that you want to apply when packets are coming in from this interface.

Egress (Outbound) Classifiers

Select from the list of existing MF Classifiers the MF Classifier that you want to apply when packets are going out of this interface.

Traffic Conditioning

Use the list box to enable or disable Traffic Conditioning on this interface.

EF Shaping

Enter a value, in bps, for Expedited Forwarding (EF) Shaping. Shaping is a process of delaying the packets in a stream in order to conform to a defined traffic profile, in this case, the EF Shaping value. Nonconforming traffic is delayed, not dropped.

Traffic Conditioning Meter Settings

Traffic conditioning is the process of dropping and remarking a traffic stream in order to shape it into compliance with a traffic metering profile.

For Expedited Forwarding (EF) and Assured Forwarding 1, Assured Forwarding 4 (AF1-AF4), you can configure a Traffic Conditioning Meter (in bps). For EF, the rate is used as an average rate, though at times traffic can burst as much as twice the configured rate. Traffic below the rate is forwarded; traffic above the rate is dropped.

For AF1-AF4, any packets under the rate are marked as low drop precedence. Any packets under two times the configured rate are marked as medium drop precedence. Any packets above two times the configured rate are marked as high drop precedence.

Egress (Outbound) Queueing Mode

The Egress Queueing Mode screen appears when you click the Configure button in the DiffServ section of the QoS Interfaces screen. Use this screen to configure egress queueing mode settings for the selected physical interface.

Figure 86 QoS Interfaces→Egress Queueing Mode



Queueing Mode

Select the Queueing mode for this interface, either DiffServ Per-Hop Behavior or Legacy Forwarding Priority.

Legacy Forwarding Priority provides backward compatibility for earlier versions of the switch.

Interface QoS Statistics

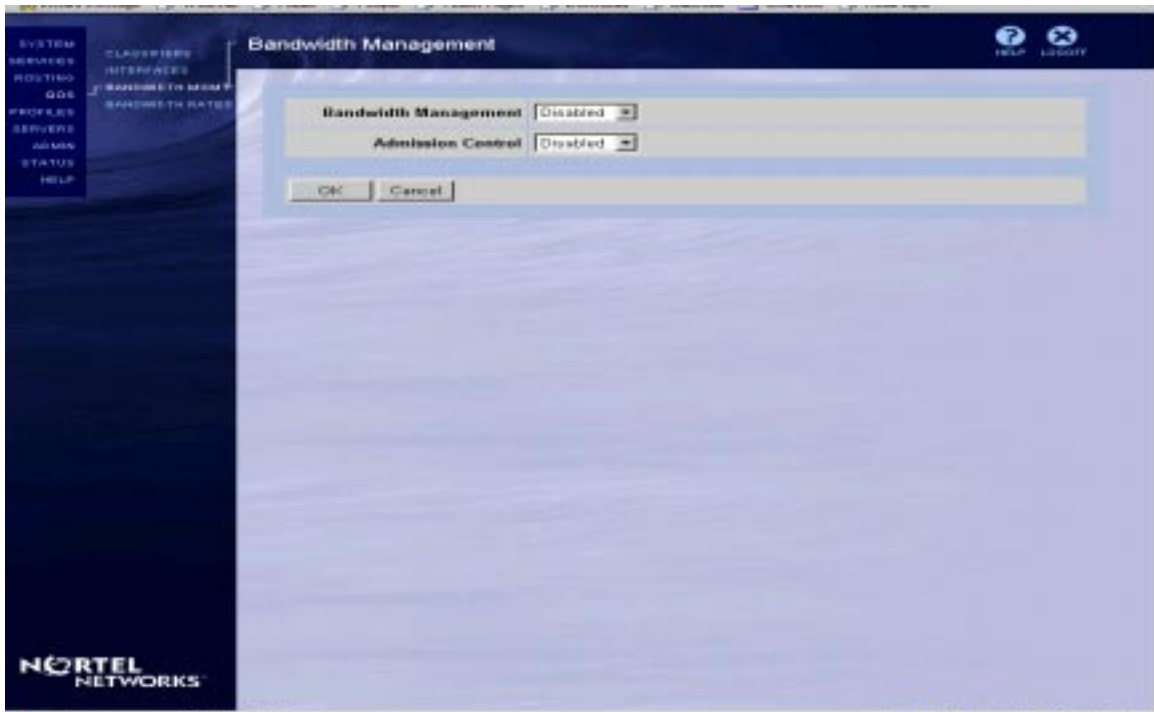
The Interface QoS Statistics button in the QoS Interfaces screen provides access to operational statistics for the interface.

Bandwidth Management

The switch's Bandwidth Management capabilities let you manage CPU and interface bandwidth resources to ensure that tunneled sessions get predictable and adequate levels of service. Bandwidth Management enables you to configure the switch resources for users, branch offices, and interface-routed traffic. Bandwidth components keep track of and control the level of bandwidth being used on the physical interfaces and the tunnels.

Bandwidth management is configured and managed from the QoS→Bandwidth Management screen.

Figure 87 QoS Bandwidth Management



Bandwidth Management

Bandwidth Management can be enabled or disabled system-wide by selecting the desired setting from the Bandwidth Management drop-down list box.

When enabled, Bandwidth settings apply.

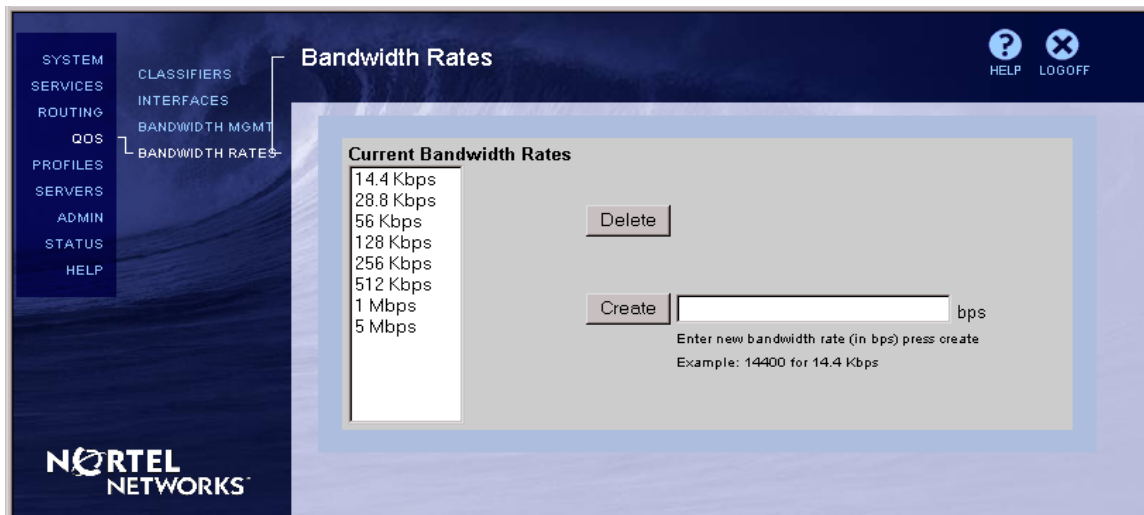
Admission Control

Admission control is a traffic control function that decides whether the switch can supply the requested bandwidth and CPU resources of a new session while continuing to provide the bandwidth and CPU resources requested by previously admitted sessions. Admission Control is used in conjunction with bandwidth policies to limit the number of concurrent user and branch tunnels.

Bandwidth Rates

The Bandwidth Rate screen allows you to manage available bandwidth rates.

Figure 88 Bandwidth Rates



Current Bandwidth Rates

The Current Bandwidth Rates list shows all existing bandwidth rates. You can delete an existing bandwidth rate or create a new bandwidth rate.

Delete

Select from the list of Current Bandwidth Rates and click delete to remove a bandwidth rate. A confirmation screen appears, prompting you to confirm that you really want to delete the selected bandwidth rate.

Create

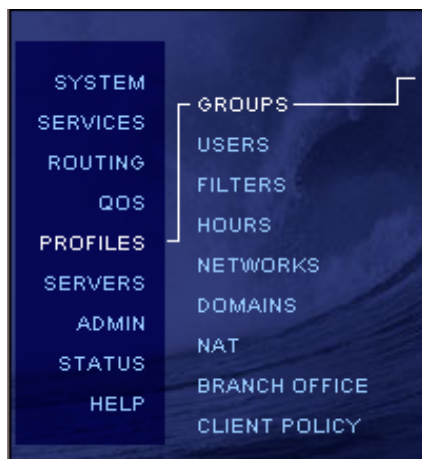
Enter a bandwidth rate (in bits per second) and click Create to create a new bandwidth rate. The new bandwidth rate is added to the list of Current Bandwidth Rates.

Chapter 5

Profiles

The Profiles menu provides access to screens that allow you to configure such things as users, user groups, branch office connections, and so forth.

Figure 89 Profiles Menu



Groups

All remote users serviced by the Switch are associated with a Group, which dictates the attributes that are assigned to a remote user session.

Groups are organized in a hierarchical manner. At the top of the hierarchy is the Base Group. The Base Group, which might be called “My Company,” contains the default characteristics that each new group inherits. Additional groups are added to the hierarchy as children of the Base Group.

The Switch authenticates each user that attempts to connect to the Switch by checking the User ID (UID) and Password against a database. The Switch supports both LDAP and Remote Access Dial-In User Session (RADIUS) databases for authentication. When using LDAP for authentication, the user is always assigned to a group since LDAP also contains the user, group, and attribute information.

When authenticating a Point-to-Point Tunneling Protocol (PPTP) client against a RADIUS database, the group for a user requesting a session is returned from the RADIUS server as a RADIUS class attribute.

In addition to assigning users to groups and providing authentication access, other group characteristics that you can configure include:

- Access hours
- Call admission priority
- Forwarding priority
- Connectivity settings
- Filters
- RSVP
- Tunneling settings
- User attributes

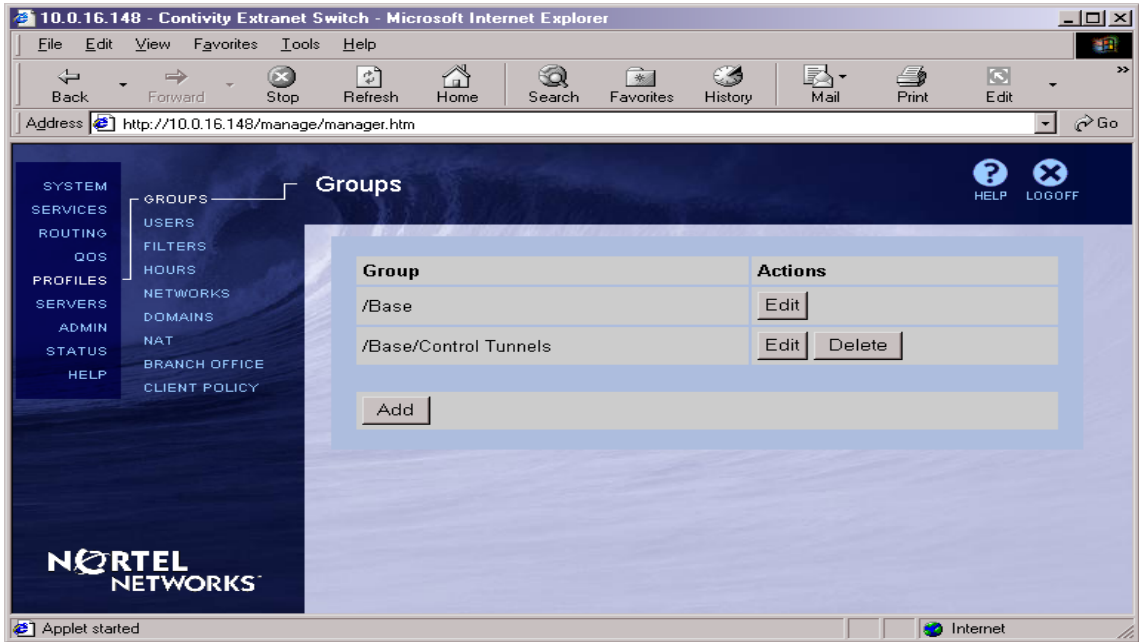
Maximum Number of Logins

The Maximum Number of Logins is not enforced across tunnel types. If you set the number of simultaneous logins to 1, a client can still get another tunnel type connection if the client is configured to use multiple tunnel types. To limit the number of connections a client can have, configure the user for a single tunnel type.

Groups screen

The Groups screen provides access to all of the groups that you want to manage with the Switch. The Groups screen allows you to change attributes that are specific to each group. Each attribute can be configured uniquely; otherwise, the attributes are automatically inherited from the parent group.

Figure 90 Groups



Group

This list box displays the current list of groups configured in the Switch. You can Add, Edit, or Delete groups using this screen.

Actions

Edit

Click Edit beside the Group name that you want to modify. The Groups Edit screen appears.

Delete

Click Delete beside the Group name that you want to remove from the database. A delete confirmation requests that you verify the deletion.



Note: You cannot delete a group that has subgroups (children) associated with it. Nor can you delete the Base Group.

Add

Click to Add a group. The Groups Add screen appears.

Add Group screen

The Groups Add screen allows you to create a new Group and associate it with a Parent Group.

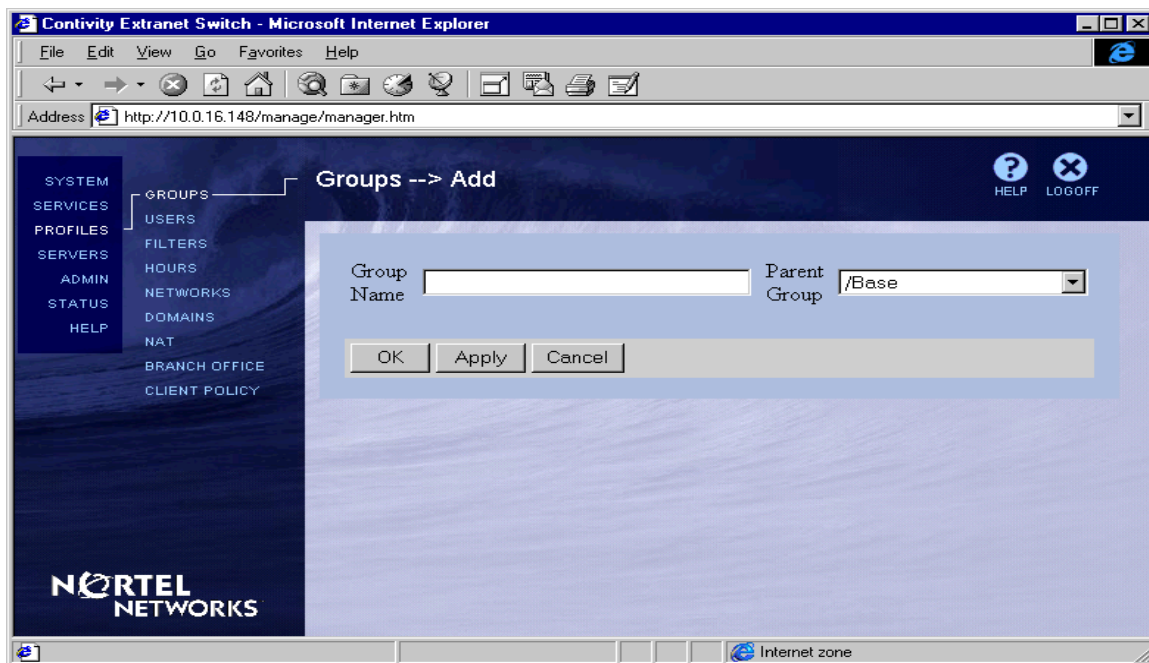
Inherited Attributes

A group inherits attributes from its parent group. For example, if the Research and Development group attributes include All Access Hours and Allow Static Addresses but deny Client-Supplied addresses, PPTP and IPSec tunneling, then the New Products (child) group would inherit these attributes.

New Attributes

You must explicitly configure a group's unique attributes to override this inheritance. You can assign a group unique network access through packet filtering, attribute support for specific tunneling technologies, minimum encryption levels, authentication mechanisms, access hours, and more.

For example, you might want to set up an Administrator group for users who are allowed to manage the Switch. This group could be configured to force tunnel connections that use encryption and strong forms of authentication, thereby improving the overall security of the Switch.

Figure 91 Groups→Add

Group Name

Enter a Group Name of up to 64 characters (spaces are permitted); for example, Research and Development.

Parent Group

The new Group is a child of the selected Parent Group. Therefore, the new group initially inherits the Parent Group's network access attributes, including authentication, tunnel types, filtering, and priorities (refer to "Edit Group" for details). Once created, these inherited options can be overwritten for the new group.

Edit a Group

The Groups Edit screen allows you to change group settings, including the main authentication, access, and connection priorities that define the group's profile.



Note: You can edit the attributes of a Group, but you cannot edit a Group name. To create a Group with the same attributes but a different name, you must add a new group and configure it with the desired attributes.

Initial Configuration

The group at the top of the hierarchy is known as the Base Group. The Base Group, due to its position in the hierarchy, contains the Switch's default values and defines the first level of inheritance.



Note: A group inherits its attributes from its Parent Group by default. You can override the default values for any attribute in any group.

Configure

Click to select an option that is different from the Parent Group (the inherited configuration).

Current Configuration

The Current Configuration shows a summary of the Group's general and tunnel configurations. Details of these listings follow in the sections on Connectivity Settings, IPSec, PPTP, L2TP, and L2F.

Figure 92 Group Configuration Edit screen (Default Attributes)

Group Name: /Base

Field	Value
Access Hours	Anytime New Hours Definition
Call Admission Priority	Highest Priority
Forwarding Priority	Low Priority
Number of Logins	1
Password Management	Disabled
Maximum Password Age	30
Minimum Password Length	16
Alphabetic Passwords	Disabled
Static Addresses	Enabled
Idle Timeout	00:15:00
Filters	permit all New Filter
IPX	Disabled
Maximum Number PPP Links	2
RSVP	Disabled
RSVP: Token Bucket Depth	3000 Bytes
RSVP: Token Bucket Rate	28 Kbps
Address Pool Name	(None defined on this switch) New Address Pool

OK Cancel

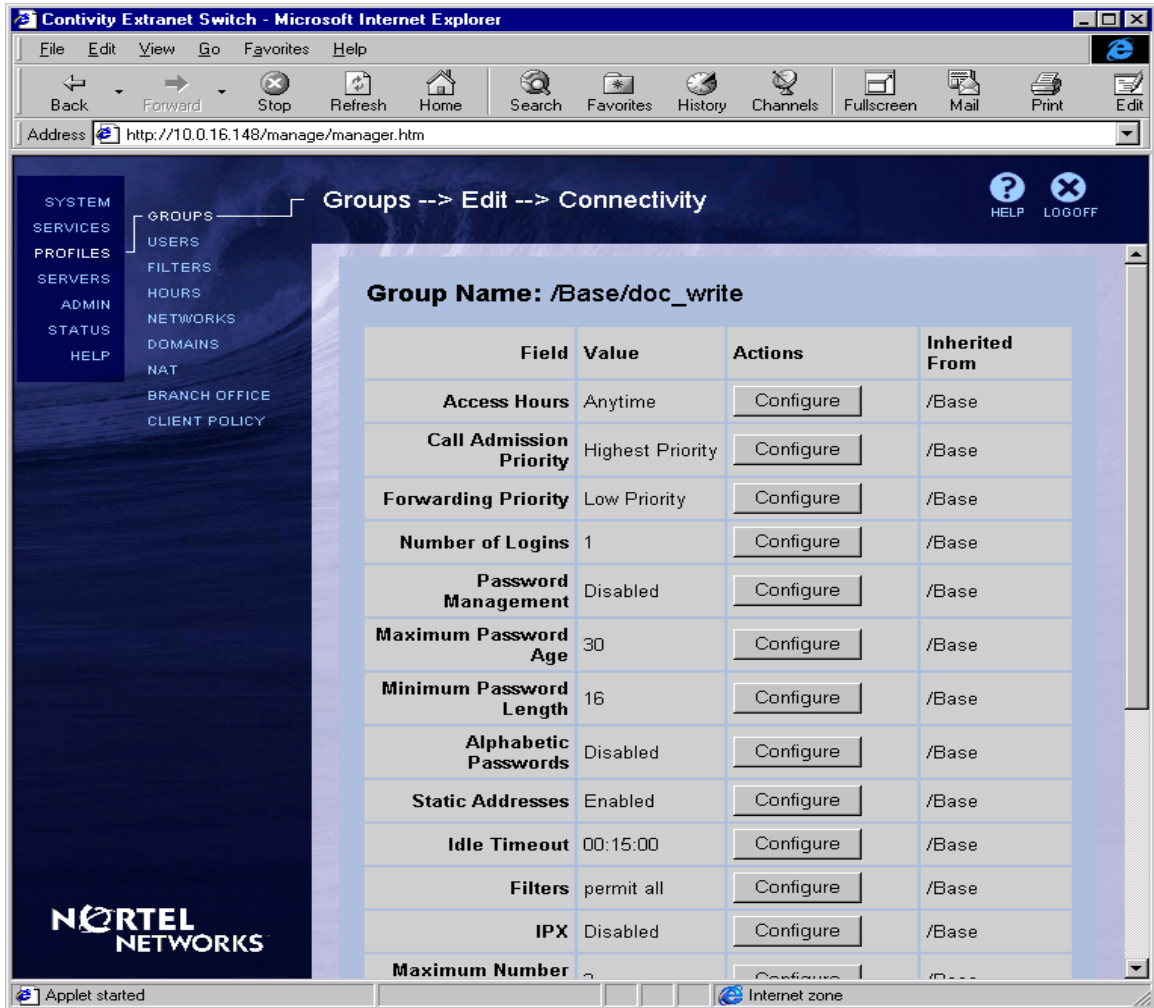
Connectivity Settings

This screen allows you to configure Group settings. The Parent group values appear by default. Click the drop-down list boxes to change values.

Contact Information

Enter the name of someone who serves as the point of contact, typically the administrator.

Figure 93 Groups Edit Connectivity



Access Hours

Specify the time ranges during which access is allowed for users in this group. These time ranges are configured from the Profiles->Hours screen. The default value is Anytime.

Call Admission Priority

Specify the Call Admission Priority level (from low to highest) you want to permit for this group. Each level is assigned a percentage of the total number of calls allowed access to the Switch. If there is a particularly high number of users logged in, new users could be denied call access, based on their Call Admission Priority, until existing callers disconnect.

Possible Call Admission Priority levels are:

- Highest Priority (default)
- High Priority
- Medium Priority
- Low Priority

Forwarding Priority

Specify the Forwarding Priority level (from low to highest) that you want to provide to sessions for users in this group. Forwarding Priority assures a certain level of latency and bandwidth allocation. For example, a group with the Highest Forwarding Priority has the highest possible bandwidth service and the lowest level of latency.

Conversely, if there is a particularly high level of traffic on the line, packets for a Low Priority group might be delayed or dropped. Since a Low Priority group has the least amount of bandwidth and the highest level of latency, some of its packets would wait until the higher priority level packets have been forwarded or they would be dropped.

Possible Forwarding Priority levels are:

- Highest Priority
- High Priority

- Medium Priority
- Low Priority (default)

Number of Logins

Click to specify the maximum number of simultaneous logins IPSec clients in the group are allowed.

Password Management

Click to enable the *Password Management facilities*, including Maximum Password Age, Minimum Password Length, and allow Alphabetic Passwords only.

Maximum Password Age

Enter the Maximum Password Age after which the login password expires. The Maximum Password Age range is from 0 (no password expiration) to 180 days (6 months). Default is 30 days. Users receive a warning that the password will expire each time they log in for two days prior to the expiration date. They also receive three warnings before access is denied.



Caution: If your clients are using a Microsoft Dial-Up Networking connection instead of the Nortel Networks Connection Manager, then they are not be notified of a password expiration or be given the opportunity to change the password prior to expiration. You should not use this feature unless you also plan to distribute the Connection Manager.

Minimum Password Length

Enter the Minimum Password Length, which can be from 3 to 16 alphanumeric characters. If you set the minimum length to eight characters, then the remote user must use at least eight characters as the login password. Default is 16 characters.

Alpha-numeric Passwords

Click to enable this feature. This forces remote users to log in with a combination of alphabetic (A to Z) and numeric (1 to 9) characters. Nortel Networks does not recommend using all alphabetic characters because this makes it easier for hackers to decode. Default is Disabled.

Static Addresses

Click to Enable Static Addresses. A Static Address allows a user to always use a specific address when logging in to the Switch. Since each user needs a unique address, the actual address is configured as part of the user profile. Disabling Static Addresses causes the Switch to ignore configured addresses in the user profile for a given group. After the client-specified address, a Static Address is the second choice. If a remote user is using a static IP address as configured on the User's screen, then this user is limited to one login.

Idle Timeout

Enter an appropriate Idle Timeout in days, hours, minutes, and seconds format: dd:hh:mm:ss. The *Idle Timeout* is an amount of time a connection can be idle (no data has been transmitted or received through the connection for the specified amount of time). When the Idle Timeout expires, the session is terminated. This option helps prevent allocation of resources on the Switch for sessions that are no longer active.

The default Idle Timeout is 00:15:00 minutes; the range is 00:00:00 to 23:59:59. The maximum number of days is 29. A setting of 00:00:00 specifies no Idle Timeout.



Note: All sessions check their configuration at startup time. Therefore, if you change the time of the idle timeout during a session, the change only affects new sessions and not any existing ones.

Filters

Select the filters you want from the pull-down list or use the default filters. The filters that appear in the drop-down list box are created using the Create Filter screen or have been supplied by Nortel Networks. Packet filtering controls the type of access allowed for users in a group, based on various parameters, including Protocol ID, Direction, IP addresses, Source, Port, and TCP Connection Establishment.

IPX

Click the drop-down list box to enable IPX support for the group.

Maximum Number PPP Links

The Switch's Multilink PPP (MP) implementation allows tunneling multilink connections to the Switch when the tunneling is being done by the ISP. Enter the Maximum Number of PPP Links that you want the Switch to support. The range is 1 to 5; default is 1.

RSVP

Click to enable RSVP (Resource ReSerVation Protocol). The Nortel Networks RSVP implementation allows you to signal the network for required bandwidth. The client must be configured appropriately for RSVP to work. Additionally, only the controlled load-service is supported. This option is Disabled by default.

RSVP: Token Bucket Depth

The Token Bucket Depth influences packet flow delays within the Switch and participating routers in the Internet. The largest amount of data the Switch holds in its queue determines latency. New packets arriving are delayed by a time that is proportional to the amount of traffic that is ahead of them in the queue, which is no greater than the Token Bucket Depth. When the queue exceeds the Token Bucket Depth, incoming packets are dropped. To guarantee reduced latency, the Bucket Depths should be small. Typically, you should not change this setting. Default is 3000 bytes.

RSVP: Token Bucket Rate

The Token Bucket Rate is the highest long-term average data rate (in Kbps) required over time for the connection. It informs the Switch and participating routers in the Internet how much bandwidth to reserve for the RSVP session. Typically, you should not change this setting. Default is 28 Kbps.

Address Pool Name

Click on the drop-down menu to select the Address Pools used by remote users to access this Switch. The drop-down list shows all pools that have been defined on the Switch. (Address pools are defined on the Servers→User IP Addr screen).

Select the New Address Pool link to define a new pool. Refer to “Remote User IP Address Pool” for details. This option is set to Default Pool by default.

User Bandwidth Policy

Click the Configure button in the User Bandwidth Policy section to modify bandwidth characteristics for this group. Click the Use Inherited button to apply the settings of the parent group to this group.

Committed Rate

Select a Committed Rate from the list of available bandwidth rates. If the desired bandwidth rate is not listed, click on Define new bandwidth rate to create a new one.

Excess Rate

Select an Excess Rate from the list.

Excess Action

Choose an Excess Action for traffic handling, either Drop or Mark.

IPSec Settings

Click the Configure button in the IPSec section to modify IPSec (Internet Protocol Security) characteristics for this group. The IPSec Edit screen appears.

The IPSec standard defines a set of security protocols that authenticate IP connections and add confidentiality and integrity to IP packets. IPSec packets are transparent to applications and the underlying network infrastructure. IPSec supports multiple encryption and authentication protocols so that your security policy can dictate levels of data privacy and authentication.

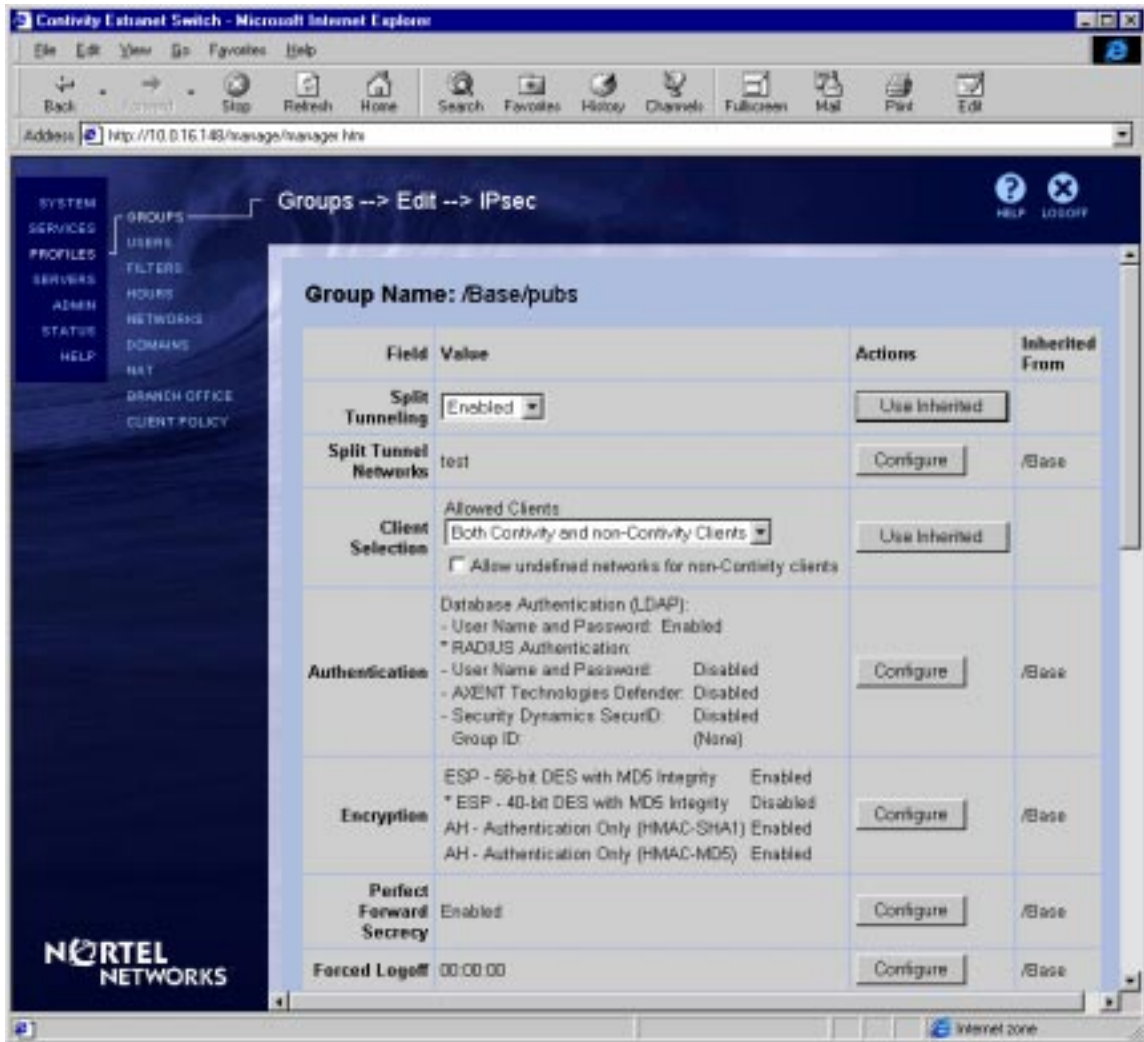
IPSec allows for multivendor interoperability. It uses a flexible key management scheme called the Internet Security Association Key Management Protocol (ISAKMP), which enables peer connections to quickly and dynamically agree on compatible security and connection parameters (keys, encryption, and authentication).

The following sections describe the fields that are unique to the IPSec screen. fields that are common to other tunneling types appear in the section Common Tunnel Settings.”



Note: Fields on the IPSec Edit screen that are preceded by an asterisk are proprietary features that apply to the Contivity VPN Client only. These fields are not used for non-Contivity clients.

Figure 94 Partial IPSec Edit



Split Tunneling

All IPSec client traffic is tunneled through the Switch by default. Split Tunneling allows you to configure specific network routes that are downloaded to the client. Only these network routes are then tunneled; any other traffic goes to the local PC interface. Split tunneling allows you to print locally, for example, even while you are tunneled into the Switch.

Unauthorized Access Prevention and Split Tunnels

The Switch takes precautions against unauthorized users potentially hacking tunneled information when the Switch is operating in Split Tunnel mode. The primary precaution in this release is to drop packets that do not have the IP address that is assigned to the tunnel connection as its source address. For example, you establish a PPP dial-up connection to the Internet with an IP address of 192.168.21.3. When you start the tunneled connection to a Switch, you are assigned a tunnel IP address of 192.192.192.192. Any packets that attempt to pass through the tunnel connection with a source IP address of 192.168.21.3 (or any address other than 192.192.192.192) are dropped. Furthermore, you can enable filters on the Switch to limit the protocol types that can pass through a tunneled connection. To completely eliminate security risks, you should not use the Split Tunneling feature.

Split Tunnel Networks

Click to select one of the networks to which you want to send encrypted tunnel traffic only. These networks are designated from the Profiles→Networks screen.

Client Selection

The Client Selection feature enables you to configure your switch to accept tunnel connections from third-party clients, in addition to the Nortel Networks Contivity VPN Client. Refer to the Contivity VPN Release Notes for a list of supported third-party clients.

Configuring for Both Contivity and non-Contivity Clients

If you choose this selection, the Switch provides support as described in the two previous sections, depending upon the type of client being used. For example, if you enable RADIUS Authentication, it is only used for Contivity clients, and you must have either preshared keys or RSA digital signature authentication enabled for non-Contivity clients.

Allowed Clients

Use the menu to specify the type of clients that are allowed to create tunnels to your switch.

Allow undefined networks for non-Contivity clients

Enabling this selection allows supported third-party clients to create IPSec tunnels to any internal networks. Nortel Networks recommends that you not allow undefined networks for third-party clients, and use Split Tunneling instead. This selection is ignored for Contivity clients.

Authentication

Authentication is performed with a protected User ID and Password through the ISAKMP key management protocol. When you click configure, the Group Security Credentials (RADIUS) dialog box appears.

Database Authentication (LDAP)

User Name and Password

Click to enable the LDAP User Name and Password to authenticate user identity. Authentication is performed with a protected User ID and Password through the ISAKMP key management protocol.

RSA Digital Signature

Click to enable the Entrust certificate authentication. You must then click the drop-down list box to choose a Default Server Certificate. Servers are configured from the System→Certificates screen.

RADIUS Authentication

The following attributes are associated with RADIUS Authentication when using IPSec tunneling. This is a two step process where (1) the Switch authenticates the remote user with the User Name and Password authentication mechanism, AXENT or SecurID hardware or software tokens, and (2) the client uses the Group ID and Group Password to authenticate the Switch's identity.

User Name and Password

Click to enable the RADIUS User Name and Password to authenticate user identity. Authentication is performed with a protected User ID and Password through the ISAKMP key management protocol.

AXENT Technologies Defender

Click to enable the AXENT OmniGuard/Defender challenge response token security authentication. The AXENT OmniGuard/Defender uses a personal identification number (PIN) and password, coupled with a challenge response security dialog, to authenticate user identity.

Security Dynamics SecurID

Click to enable the Security Dynamics SecurID token security authentication. The SecurID uses a PIN and the current code generated by a token assigned to the user to authenticate user identity.

Group ID and Password

Enter the Group ID and Password, which are encrypted for transmission.

Group ID

Enter the Group ID, which provides access to the Switch. Subsequent LDAP and RADIUS authentication is verified against the User ID.

Group Password

Enter the Group Password, which provides access to the Switch. Subsequent LDAP and RADIUS authentication is verified against the User Password.

Group Confirm Password

Reenter the Group Password.

Encryption

Click Configure, then click the appropriate checkbox to either enable or disable the supported Encryption methods for this group.



Note: Using higher-level encryption, such as Triple DES, decreases performance.

The encryption methods are presented in order of strength, from strongest to weakest. All of the following encryption methods ensure that the packet came from the original source at the secure end of the tunnel. Some of the encryption types do not appear on non-US models that are restricted by US Domestic export laws. Also, MD5 (Message Digest) provides integrity that detects packet modifications.

ESP – Triple DES with MD5 Integrity: Encapsulated Security Payload Triple DES (Data Encryption Standard) uses the same principle as DES (below), but uses a 168-bit key. It uses the DES encryption algorithm three times. The first 56 bits of the key is used to encrypt the data, then the second 56 bits is used to decrypt the data. Finally, the data is encrypted once again with the third 56 bits, which triples the algorithm's complexity.

ESP – 40- or 56-bit DES with MD5 Integrity: Encapsulated Security Payload Data Encryption Standard (DES) is an encryption block cipher algorithm. DES uses a 40- or 56-bit key (with 8 bits of parity) over a 64-bit block. The 40 or 56 bits of the key are transformed and combined with a 64-bit message through a complex process of 16 steps.

Both 40- and 56-bit DES require the same processing demands, so you should use 56-bit DES unless local encryption laws prohibit doing so.

AH – Authentication Only (HMAC-SHA): The Authentication Header Message Authentication Code Secure Hash Algorithm (HMAC-SHA) produces a 160-bit hash. It is regarded by cryptographers as being more resistant to attacks than MD5. It does not encrypt data.

AH – Authentication Only (HMAC-MD5): The Authentication Header Message Authentication Code Message Digest 5 (HMAC-MD5) Algorithm is used to confirm the authenticity of a packet. It produces a 128-bit hash. It does not encrypt data.

If two devices have different encryption settings (due to either US export laws or administrative configuration), the two devices negotiate downward until each has a compatible encryption capability. For example, if a client in the US attempts to negotiate Triple DES encryption with a Switch in Australia, then the Australian Switch rejects Triple DES encryption in favor of DES.

IKE Encryption and Diffie-Hellman Group

Select the Diffie-Hellman Group level to apply to IKE (Internet Key Exchange) encryptions.



Note: The choice of the IKE encryption algorithm does not affect the choice of the encryption algorithm used to encrypt data in IPSec. For example, one can use DES to encrypt the IKE exchanges, and then negotiate Triple DES for use in IPSec.

The Services→IPSec screen contains a section labeled “IKE Encryption and Diffie-Hellman Group.” This section provides two choices for use with IPSec.

Perfect Forward Secrecy

Click to enable Perfect Forward Secrecy (PFS). With PFS, keys are not derived from previous keys. This ensures that one key being compromised cannot result in the compromise of subsequent keys.

Forced Logoff

For IPSec tunneling, you can specify a time after which all active users are automatically logged off. The default is 0, which means the option is turned off. The possible range is 00:00:01 to 23:59:59.

Client Auto Connect

The Client Auto Connect feature enables remote Contivity VPN Clients to connect their IPSec tunnel sessions in a single step. This is similar to the way Microsoft's Dial-Up Networking automatically connects to an ISP when a Web browser is launched. With Auto Connect, client users simply click on the desired destination, for example, a Web page on the private internal network. This first starts their dialup connection, then makes the tunnel connection to the Switch, and finally makes the connection to the requested destination. What has, in the past, taken three distinct user operations is now accomplished by a single action.

Enabled

Click to enable the Client Auto Connect feature on the Switch.

Any Network Traffic

Click on this selection to use the autoconnect feature for all client connection requests to authorized destinations. Now, when any network activity is detected on the user's workstation, a tunnel connection is automatically launched to the Switch. In this manner, the Client Auto Connect feature works like Microsoft's Dial-Up Network Auto Dial feature.

Specify Networks and/or Domains

Click on this selection to limit autoconnection use to specific domains or networks. Specify the authorized domains or networks in the following two fields.

Domains

Use this selection to designate specific domains or hostnames that trigger the autoconnect feature. The domains that you specify must be configured on the Profiles→Domains page (refer to Domains"). Select None if you want to limit the autoconnection feature to specific networks, which you specify in the following Networks field.

Networks

Use this selection to designate specific networks that trigger the autoconnect feature (the networks must be configured on the Profiles→Networks page). Select None if you do not want to designate any networks.

Banner

You can customize an enterprise login banner for the Contivity VPN Client by entering text into the space provided. This banner appears at the top of the IPSec client upon login.

Display Banner

Click to enable the banner and have it appear when a remote user logs into the Switch.

Client Screen Saver Password Required

Setting this security feature forces the client to use a password in association with a screen saver. When enabled, if the user leaves the system and is connected to a tunnel, the system then gets locked out of the tunnel once the screen saver kicks in.

The end user would enable this feature from the Start→Settings→Control Panel→Display→Screen Saver Password Protected checkbox. Default is Disabled.

Client Screen Saver Activation Time

This setting is used together with the Client Screen Saver Password Required setting. It defines the maximum time (in minutes) before the client's screen saver is activated. The value on the Client PC can be changed from the Start→Settings→Control Panel→Display→Strengthen Wait list box. Default is 5 Minutes.

Client Fail-Over Tuning

Enabled

Check this box to enable client fail-over. Client fail-over uses small packets to check and maintain, or keep alive, the connection between the client and the Switch.

Interval

In the Interval section, specify the time interval that the client waits between VPN activity checks.

Nortel Networks recommends a low interval when users are connecting via the client. You should use a higher setting for situations such as when a lease line is used and charges are based on traffic.

Maximum Number of Retransmissions

Specify the maximum number of retransmissions in this field. This is the number of times that the client re-transmits a keepalive packet to the Switch to check for connectivity.

Allow Password Storage on Client

You can allow client systems to save the login password in its password list, or you can require that the remote user enters the password each time he requests authentication and access to an IPSec tunnel. Click Enable to allow client systems to save the login password.



Note: When using certificates, saving the password on the client is not allowed.

Compression

Click to enable Compression for IPSec tunneling. Refer to Compression” for details.

Rekey Timeout

You should limit the lifetime of a single key used to encrypt data or else you compromise the effectiveness of a single session key. Use the Rekey Timeout setting to control how often new session keys are exchanged between a client and a server. You should set the Rekey Timeout setting to no less than 1 hour.

Default is 08:00:00 (8 hours); a setting of 00:00:00 disables the Rekey Timeout setting. The maximum setting is 23:59:59.

Rekey Data Count

You can choose to set a Rekey Data Count depending on how much data you expect to transmit via the tunnel with a single key. Default is 0 Kbytes; a setting of 0 disables the Rekey Data Count.

Domain Name

This setting enables you to specify the name of the domain that is used while an IPSec tunnel is connected. Specifying the domain name in this field ensures that domain lookup operations point to the correct domain. This is particularly important for clients that use Microsoft Outlook or Exchange, to ensure that the mail server is mapped to the correct domain.

When a tunnel is connected, the remote client's registry is updated to use the specified domain. When the client disconnects the tunnel, the remote client's original domain is again used.

Primary DNS

See Primary DNS" in Common Tunnel Settings."

Secondary DNS

See Secondary DNS" in Common Tunnel Settings."

Primary WINS

See Primary WINS" in Common Tunnel Settings."

Secondary WINS

See Secondary WINS” in Common Tunnel Settings.”

Nortel Client Requirements

Minimum Version:

Select the minimum version of Contivity VPN Client that is required.

Action

Specify the action to take upon detection of a noncompliant client.

Message:

Type a message giving users the URL for a Web site or FTP site from which they can download the required version of the Contivity VPN Client software.

Filter:

Select a filter to apply from the list of available filters.

New Filter

Click on the New Filter link to go to the screen and create a new filter.

Client Policy

Select a client policy as appropriate. Client Policy helps prevent potential security violations that could occur when you are using the split tunneling feature. Split tunneling allows client data to travel either through a tunnel to the enterprise network or directly to the Internet. Refer to Client Policy” for additional information.

Allow IPSec Data Protection

Enable or disable IPSec.

PPTP

Click to modify Point-to-Point Tunneling Protocol (PPTP) characteristics for this group. The PPTP Edit screen appears.

PPTP is a tunneling protocol supported by Nortel Networks, Microsoft, and other vendors. The PPTP client is available for Windows 95 (www.microsoft.com) and is built-in to Windows 98 and Windows NT. PPTP supports multiple authentication schemes: MS-CHAP, CHAP, or PAP. Additionally, you can enable compression, RC4-based encryption, and assign DNS and WINS servers to the tunnel. Refer to Common Tunnel Settings” for additional information.

Figure 95 PPTP Edit

Groups --> Edit --> PPTP

Group Name: /Base/doc_write

Field	Value	Actions	Inherited From
Authentication	MS-CHAP: V1, V2, Not Encrypted, RC4-40 CHAP: Enabled PAP: Disabled (NOTE: PAP passwords are sent in the clear)	Configure	/Base
Compression	Enabled	Configure	/Base
Use Client Specified Address	Disabled	Configure	/Base
Primary DNS	(None)	Configure	/Base
Secondary DNS	(None)	Configure	/Base
Primary WINS	(None)	Configure	/Base
Secondary WINS	(None)	Configure	/Base
All Fields		Configure Use Inherited	

OK Cancel

NORTEL NETWORKS

L2TP

Click to modify L2TP (Layer 2 Tunneling Protocol) characteristics for this group. The L2TP Edit screen appears.

L2TP is a tunneling protocol supported by Nortel Networks, Cisco Systems, Microsoft, and other vendors. L2TP combines the best features of the L2F and PPTP tunneling types. L2TP tunneling enables secure remote access to enterprise networks across the public Internet. L2TP tunnels are generally established between a network access server (NAS) at the Internet Service Provider (ISP) and the Switch.

L2TP allows you to specify MS-CHAP, CHAP, or PAP authentication, enable compression, and assign DNS and WINS servers to the tunnel. The following sections are specific to L2TP over IPSec tunnels. Refer to Common Tunnel Settings” for additional information about other settings.

L2TP/IPSec Data Protection

Select the level of protection to apply to the tunnel.

Require IPSec Transport Mode Connections

Specify the group from which this tunnel gets credentials.

Figure 96 L2TP Edit

10.0.16.148 - Contivity Extranet Switch - Microsoft Internet Explorer

Address: http://10.0.16.148/manage/manager.htm

Groups --> Edit --> L2TP

Group Name: /Base

Field	Value
Authentication	MS-CHAP: ☒ V1 ☒ V2
	☒ Not ☒ RC4- ☒ RC4-128
	Encrypted 40
	CHAP: ☒
	PAP: ☐
(NOTE: PAP passwords are sent in the clear)	
Compression	Enabled
Use Client Specified Address	Disabled
Primary DNS	
Secondary DNS	
Primary WINS	
Secondary WINS	
L2TP/IPsec Data Protection	Not Required
Require IPsec Credentials From Group	/Base

OK Cancel

NORTEL NETWORKS

L2F

Click to modify L2F (Layer 2 Forwarding) characteristics for this group. The L2F Edit screen appears.

L2F is a tunneling protocol supported by Nortel Networks, Cisco, Shiva, and other vendors. L2F tunneling enables secure remote access to enterprise networks across the public Internet. L2F tunnels are generally established between a network access server (NAS) at the Internet Service Provider (ISP) and the Switch.

L2F allows you to specify a CHAP or PAP authentication scheme, enable compression, and assign DNS and WINS servers to the tunnel.

Refer to Common Tunnel Settings” for additional information.

Figure 97 L2F Edit

Contivity VPN Switch - Microsoft Internet Explorer

Address: http://10.0.16.148/manage/manager.htm

Groups --> Edit --> L2F

Group Name: /Base/doc_write

Field	Value	Actions	Inherited From
Authentication	CHAP: PAP: (NOTE: PAP passwords are sent in the clear)	Enabled Disabled Configure	/Base
Compression	Enabled	Configure	/Base
Use Client Specified Address	Disabled	Configure	/Base
Primary DNS	(None)	Configure	/Base
Secondary DNS	(None)	Configure	/Base
Primary WINS	(None)	Configure	/Base
Secondary WINS	(None)	Configure	/Base
All Fields		Configure Use Inherited	

OK Cancel

NORTEL NETWORKS

Common Tunnel Settings

Authentication

Select one or more of the PPTP/L2TP/L2F Authentication methods. These methods are Enabled by default.

- MS-CHAP – Click to enable Microsoft encrypted authentication for PPTP and L2TP only.

Windows NT, Windows 98, and Windows 95 clients can negotiate PPP connections using MS-CHAP as the authentication algorithm. This is the Microsoft version of CHAP; it is a secure form of authentication.

Associated with MS-CHAP authentication are the following optional encryption levels for preserving the privacy of tunneled traffic. These encryption levels are valid for PPTP tunnels only.

Data Encryption

Click to enable acceptable level(s) of data encryption for MS-CHAP.

- Not Encrypted– Tunnels requesting no data encryption are accepted.
- RC4-40 – Tunnels requesting 40-bit RC4 encryption are accepted.
- RC4-128 – Tunnels requesting 128-bit RC4 encryption are accepted. This is the most secure method. The longer the encryption key, the more secure the encryption. US export law controls the export of 128-bit encryption keys.

If two devices have different encryption settings (due to either US export laws or administrative configuration), the two devices negotiate downward until each has a compatible encryption capability. For example, if a client in the US attempts to negotiate RC4-128 encryption with a Switch in Ireland, then the destination Switch rejects RC4-128 encryption in favor of RC4-40.



Note: You can only use Microsoft Point-to-Point Encryption (MPPE) when using MS-CHAP authentication

- **MS-CHAP Version 2** – Microsoft Challenge-Handshake Authentication Protocol Version 2 (MS-CHAP-2) is a Microsoft proprietary Point-to-Point authentication protocol that provides LAN-based users the same functionality as Version 1 and includes bidirectional authentication. Additionally, MS-CHAP-2 integrates the encryption and hashing algorithms used on Windows networks.
- **CHAP** – Click to enable Challenge Handshake Authentication Protocol (CHAP) encrypted password authentication. CHAP provides protection for passwords, but no data encryption.
- **PAP** – Click to enable Password Authentication Protocol (PAP) authentication. Neither the password nor the data is protected.

Compression

Click to enable the IPsec HI/fn LZS compression or the PPTP, L2TP, or L2F Microsoft Point-to-Point Compression (MPPC) packet compression. Compression should be used when encryption is selected on analog modems. This is because encryption renders a modem's compression ineffective, and it can severely affect the performance of compressible applications. Also, data that is compressed before being transmitted makes more efficient use of lower speed network links.

You should use data compression in most typical situations. Users with cable modems or xDSL connections to the ISP, or locally on the LAN, would find it is probably unnecessary to compress packets. This is because the speed of the link, relative to the rate of compression and the benefit of compressing before encrypting, might be negligible or might not increase performance.

Also, some data cannot be compressed; for example, a previously compressed file does not lend itself well to additional compression.

Use Client-Specified Address

Click to enable use of a Client-Specified Address. This option allows the Switch to accept the IP address from a remote user's system during tunnel setup. This option is Disabled by default.

When enabled and the client provides an IP address, this is the IP address that is used by the client for the duration of the tunneled session (it becomes the first or default choice).

Common DNS and WINS Server Fields

The following DNS and WINS server fields are common to all tunnel types.

Primary DNS

Enter the address of the Primary Domain Name System (DNS) server that is located on your private network. This DNS address is provided by the server to tunnel clients at setup and is used through the tunnel. The DNS server translates textual host names into IP addresses for the Switch. For example, DNS can translate the fully qualified host *www.mycompany.com* to its IP address 192.19.2.33.

The Primary DNS server is the first one addressed for servicing name resolution requests from a remote user; if the Primary DNS server is unavailable, service is requested of the Secondary DNS server. Recent versions of Microsoft Windows operating systems can simultaneously query multiple DNS servers.

Always use the IP address for setting a DNS server host instead of a domain name.

Secondary DNS

Enter an address for the Secondary Domain Name System (DNS) server. If the Primary DNS server is unavailable, service is requested of the Secondary DNS server.

Primary WINS

Enter an address for the primary Windows Internet Naming Service (WINS) server. A WINS server resolves NetBIOS names (for Windows networking file and print services) to IP addresses. Using a WINS server enables normal Windows file and print services to be accessed correctly through a tunnel connection.

Windows NT Server Version 4.0 and later supports a built-in WINS server. The WINS server eliminates the need to manually map NetBIOS names to IP addresses (for example, using the textual LMHOSTS file on Windows) by updating a name-to-address mapping file dynamically on the WINS server.

The Primary WINS server is the first one addressed for servicing name resolution requests from a remote user; if the Primary WINS server is unavailable, service is requested of the Secondary WINS server. Always use the IP address for setting a WINS server host instead of a name.



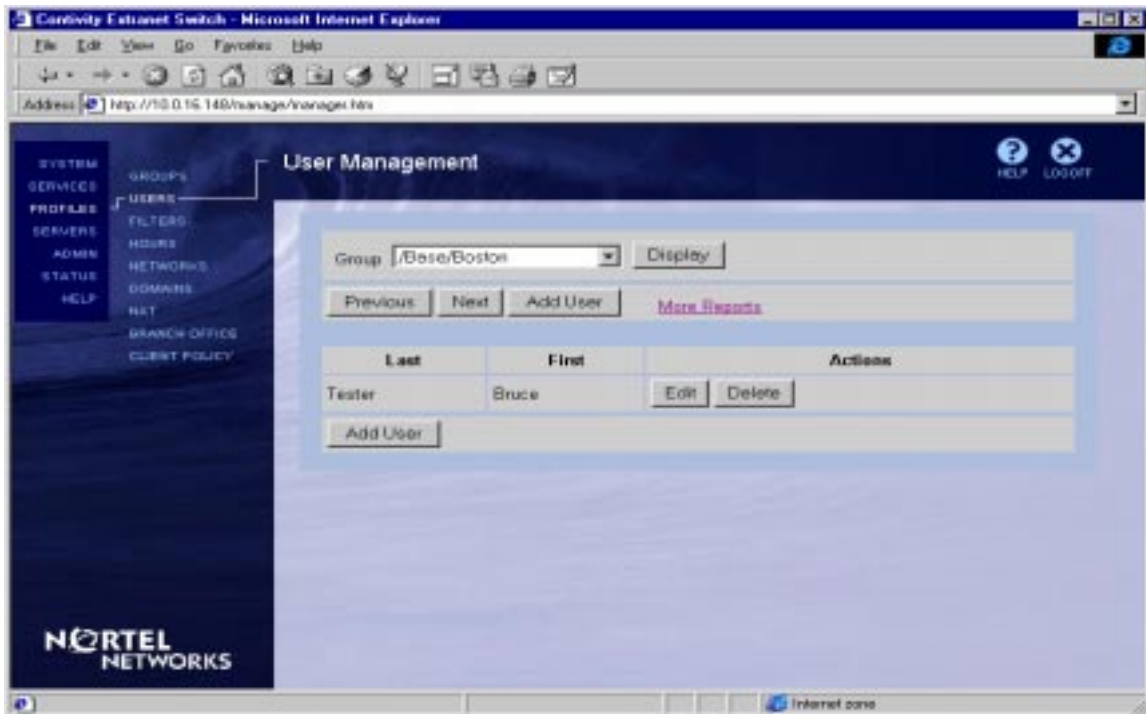
Note: If no WINS servers are specified, the client is forced to broadcast for NetBIOS names.

Secondary WINS

Enter an address for the Secondary Windows Internet Naming Service (WINS) server; if the Primary WINS server is unavailable, service is requested of the Secondary WINS server.

User Management

The User Management screen allows you to add, edit, delete, or search for a user profile in a group.

Figure 98 User Management Group Profile

Group

Select a Group to which you want to add or modify users from among those in the Group drop-down list box. If you need to add a new group, select Profiles→Groups.

Display

After selecting a Group, you must click Display to view the group members. This allows you to quickly change from viewing one group to another.

Last/First

The Last names and First names of the selected group's users appear, sorted by Last name.

Actions

Edit – Click to Edit a User Profile in the Group; the Edit User screen appears.

Delete – Click to Delete a User from the Group.

Add User

Click to Add a User to the Group; the Add User screen appears.

Search

The Search option appears only after you have six or more users in the displayed group. The Search option allows you to readily search within a selected group and then configure a specific user's account.

Select a Group from which you want to search for a particular user from the Group drop-down list box (at the top of the screen), and click Display. The search is limited to the available groups. Select one of the following as the preferred search method, then click Search.

- Last Name searches for a Last Name. You must enter the entire last name.
- UID searches for a User ID.
- Admin Rights searches for anyone who has View or Manage Administrator privileges.
- LDAP search allows you to enter any LDAP database attribute that is part of the person, organizational Person, or inetOrgPerson object database (for example, cn=common name or sn=surname) to generate the associated user's profile. Refer to your LDAP vendor's documentation for complete details.

User Add or Edit

This screen allows you to Add or Edit a User profile. A *user profile* includes User IDs (UIDs) and passwords for the various tunneling protocols, and the assignment of Administrative rights. This screen also allows for the configuration of an IP address that is always associated with the remote user.



Note: You should not add user profiles for RADIUS authenticated users. Instead, ensure that the proper User IDs and Passwords are in the external RADIUS database.

The Switch always queries the LDAP database first, and if a UID and Password combination is found it uses this rather than an external RADIUS authentication server.

Only options that are enabled for the specified group appear on this screen. Furthermore, only options that the administrator who is currently viewing the screen has rights to appear (configuration options only appear if the administrator has Manage Users and Manage Switch Administrator Rights).

Figure 99 Partial User Add or Edit

General

First

Last

Name

FirstLast

Group

/Base/Beacon

Static IP Address

Static Subnet Mask

Remote User

Note: The static IP subnet mask is used for IPsec connections only

User Accounts

	User ID	Password	Confirm Password	Expires (Days)
IPsec				
PPTP				
L2TP				
L2F				

IPsec Certificate Credentials

Remote Identity

Valid Issuer Certificate Authority

(No issuer CAs available)

Subject Distinguished Name

Relative

Common Name

Org Unit

Organization

Locality

State/Province

Country

Full

Full Distinguished Name

Subject Alternative Name

Subject Name Type

Email Name

Local Identity

Server Certificate

(No server certificates available)

Administration Privileges

	User ID	Password	Confirm Password
Admin			

Admin Rights

Manage Switch

None

Manage Users

None

/Base

OK

Cancel

Reference for the Contivity VPN Switch

You can assign a user to two different groups, but only if the user has two different User IDs (UIDs); for example, mlee and madilee. The system does not allow you to enter the same User ID in two different groups.



Note: When adding a user account, depending on the group configuration, the account can have up to four User IDs. If you are creating an enterprise User ID standard, you should try to avoid schemes that might potentially create conflicts as your company grows. For example, you should not use the person's full first name and last initial.

Name

Enter the First and Last Name of the user whose profile you want to add or change. This is the regular name associated with a person (for example, Mario Lemieux). This user can have different IDs and passwords for each tunnel type.

Group

Shows the Group to which the user belongs and its Parent group. You can move the user to a another Group by selecting a different Group name.

Remote User

Static IP Address

Enter a Remote User Static IP Address to use in place of a pool (client-specified or DHCP) server-assigned IP address. This IP address is associated with the Static IP Address option in the Groups→Connectivity option (it is only used if the group allows it).



Note: If an IP address that is entered here is used instead of a DHCP server-assigned IP address, *then only one login is allowed.*

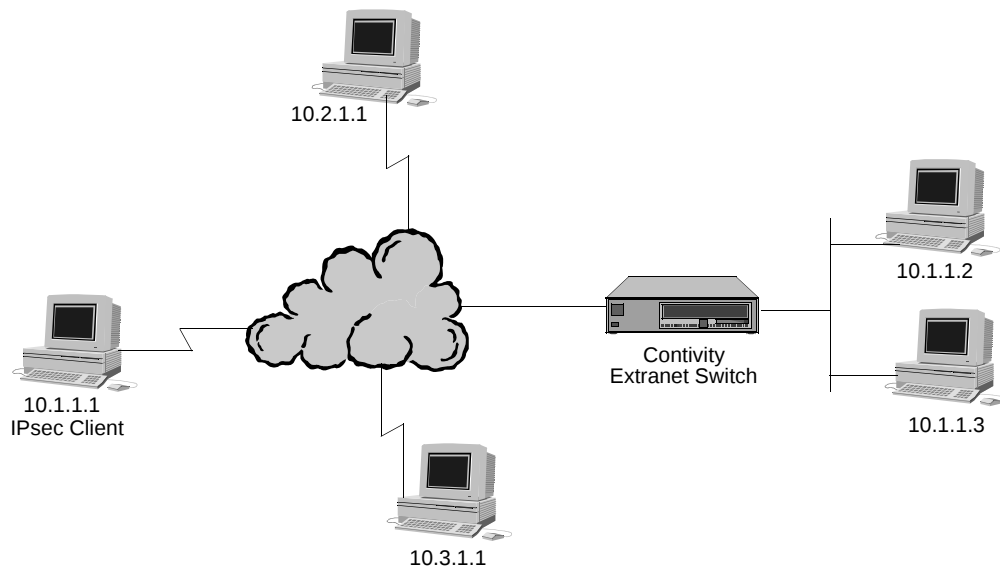
Static Subnet Mask

Assigning the correct subnet mask to a remote IPSec client is important when using Split Tunneling. When Split Tunneling is enabled, packets destined to a host listed in the Split Tunnel Network list are directed into the tunnel by the IPSec client. All other traffic goes through a standard LAN or dialup interface. This happens on the client by adding the routes listed on the Split Tunnel Network list to the route table of the Microsoft TCP/IP stack and pointing those routes to the tunnel adapter interface. A route is also added to the route table based on the subnet mask assigned to the tunnel adaptor.

Previously, there was no method to specify the subnet mask to be used on the client, so the client used the natural mask based on the class of the assigned IP address. For example, if the tunnel adaptor is assigned the address 10.1.1.1, the natural mask would be a Class A mask of 255.0.0.0. This would cause a rogue for 10.0.0.0 with a mask of 255.0.0.0 to be added to the route table and all packet destined to any address in the 10 network address space would be directed into the tunnel incorrectly.

The IPSec Subnet Mask field allows you to specifically assign a subnet mask to a remote IPSec client that obtains an IP address either from the IP Address Pool, DHCP, RADIUS, or a static user configuration.

The following illustration helps understand the specified address mask.

Figure 100 IPsec Subnet Mask Assignment

If the IPsec client established an extranet connection and was assigned the IP address 10.1.1.1 using the natural mask, a route would be added from 10.0.0.0 with a mask of 255.0.0.0 to the TCP/IP stack's route table. If the client wanted to send data to 10.1.1.2 on the remote corporate network, the packets would be directed to the tunnel adaptor correctly. But if one client wanted to send data to 10.2.1.1, which is directly accessible on the Internet, the packet would be directed into the tunnel incorrectly. By configuring a subnet mask of 255.255.0.0, a packet destined for the 10.2.1.1 network would not be directed into the tunnel and would be access directly.

User Accounts

You can establish user accounts for remote users to tunnel into the Switch through specific tunneling types, as configured here.

IPSec

Enter the User ID and Password to allow IPSec (IP security) access privileges for this user. The User ID for IPSec accounts is typically, though not required to be, a fully qualified domain name (FQDN); for example, mlemieux@penguins.com. LDAP is the only authentication server that currently supports IPSec.

PPTP

Enter the User ID and Password to allow PPTP (Point-to-Point Tunneling Protocol) access privileges for this user if you are not externally authenticating the user; otherwise, use external Authentication.

L2TP

Enter the User ID and Password to allow L2TP (Layer 2 Tunneling Protocol) access privileges for this user if you are not externally authenticating the user; otherwise, use external Authentication.

L2F

Enter the User ID including the domain (for example, bclinton@whitehouse.gov) and Password to allow L2F (Layer 2 Forwarding) access privileges for this user if you are not externally authenticating the user; otherwise, use external Authentication.

Expires (Days)

Shows the number of days remaining before the password expires. When the field says Now, then the password has already expired. You must therefore reset the Maximum Password Age setting for this user. When the field says Never, then the Maximum Password Age setting is 0, which means to never age (expire). Refer to Maximum Password Age” for additional information on the Maximum Password Age option.

IPSec Certificate Credentials

Remote Identity

Valid Issuer Certificate Authority

Select a Valid Issuer Certificate Authority from the drop-down list. These Certificate Authorities are configured from the System→Certificates: Generate Certificate Request screen.

Subject Distinguished Name

You can use either the relative distinguished name or the full distinguished name.

Relative

The relative distinguished name is a collection of the following components that uniquely identify the remote peer in an IPSec certificate environment.

Organization

Enter the Organization with which the user is associated.

Organizational Unit

Enter the Organizational Unit with which the user is associated.

Common Name

Enter the Common Name with which the user is associated.

Country

Enter the Country in which the user resides.

State/Province

Enter the State/Province in which the user resides.

Locality

Enter the Locality in which the user resides.

Full

You can directly enter the Full Distinguished Name (FDN) in this field rather than entering the individual components in the previously described Relative distinguished name fields. A sample entry follows:

```
CN=MySwitch, O=MyCompany, C=US
```

Subject Alternative Name

You can optionally use a Subject Alternative Name in place of a Subject DN, and specify the format of the name. The following formats are acceptable.

- Email Name (for example, net_admin@company.com)
- DNS Name (for example, gateway.cleveland.company.com)
- IP Address (for example, 192.168.34.21)

Local Identity

Server Certificate

Click the drop-down list box to view all certificates that have been issued to the server. Server Certificates are configured from the System→Certificates: Generate Certificate Request screen.

Administration Privileges

Administrator privileges are assigned to users in charge of configuring, monitoring, and managing the Switch. Enter the User ID and Password to allow this person Administrator Rights (and reenter the password to verify that you typed the password you intended).

Admin Rights

There are two types of Administrator access rights: Manage Switch and Manage Users. In addition to providing different levels of access rights, the Admin Rights settings also control which status reports you can view (see the section 'Status Reports' for the types of reports).

Each access right can be assigned one of the following privilege levels:

- **None** - This user does not have Administrator rights to Manage the Switch or Manager Users; the user cannot view or manage Switch Configuration or User settings.
- **View** - This user has Administrator rights to View (monitor) Switch Configuration or User Rights settings; however, the User cannot Manage (change) them. This is the lowest level of Administrator Rights.
- **Manage** - This user has Administrator rights to View (monitor) and Manage (configure) other Switch Configuration or User Rights settings. This is the highest level of Administrative Rights.

Manage Switch

This setting allows you to manage the Switch completely, including groups, servers, control settings, and encryption levels. However, to manage users, *you must also enable the Manage Users setting for this user.*

Manage Users

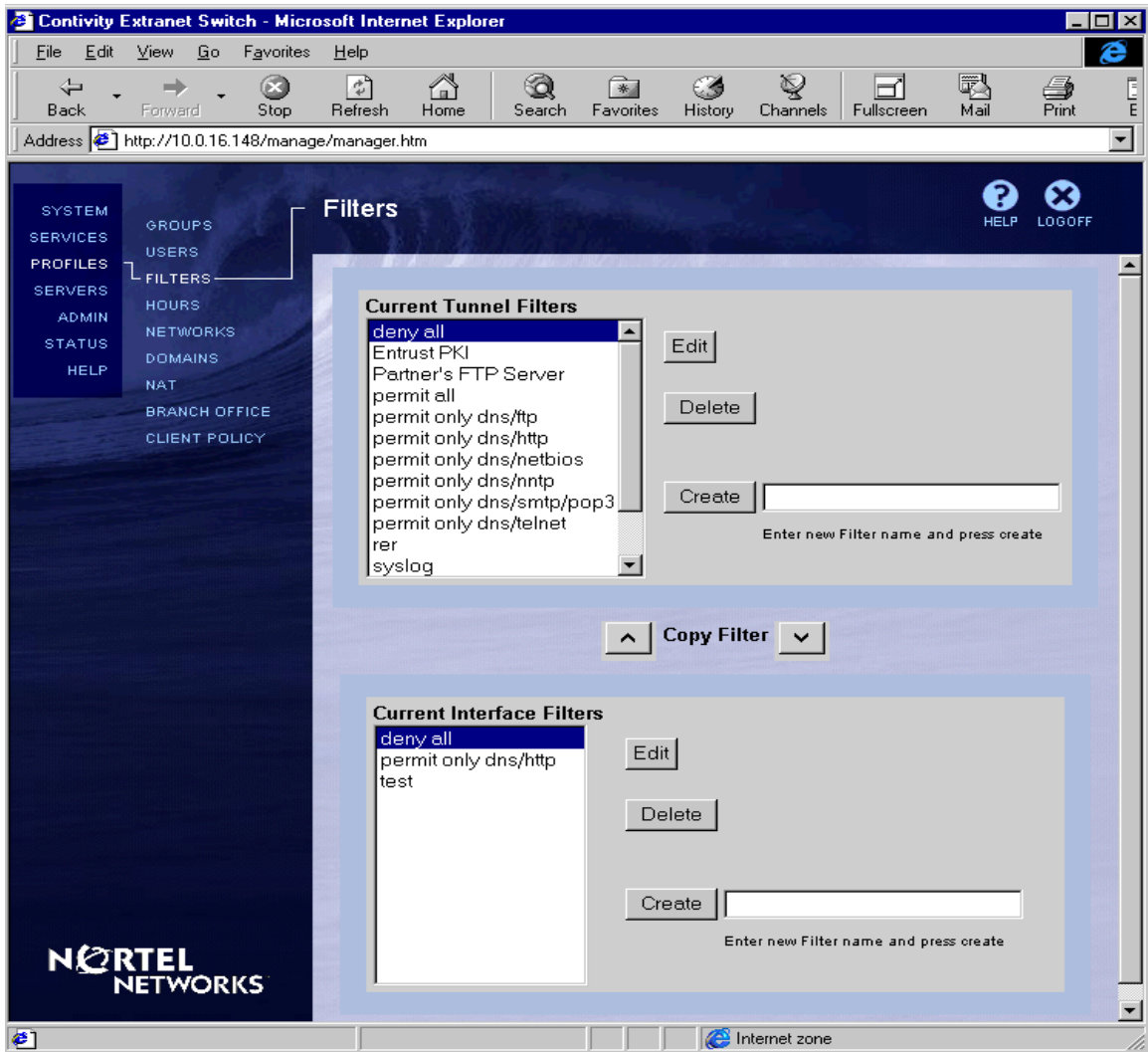
This setting allows you to Manage Users, which allows you to add, delete, or edit User records.

Next, select from the drop-down list box the groups for which this administrator can manage users.

Filters

The Filters screen allows you to Create, Modify, Copy, or Delete a Filter. You use this screen to manage your Switch's tunnel filters (for user groups) or interface filters (for LAN and WAN interfaces).

Figure 101 Filters



Changing a tunnel filter does not affect any existing tunnels. You must reestablish the existing tunnels for changes to take effect.

Current Filters

The Current Tunnel Filters and Current Interface Filters windows show the currently available filters. A filter usually consists of one or more inbound rules (coming into the enterprise) and one or more outbound rules (leaving the enterprise). Filter names are a convenient way of managing a set of rules.

To perform any of the following operations, click on the filter in the Current Filters window, then click on the appropriate button.

Edit

Click the filter that you want to modify, then click the associated Edit button. The Filter Rules for that filter appear.

Delete

Click the filter that you no longer intend to use, then click the associated Delete button. The name is removed from the list. You cannot delete a filter that is currently in use.

Create

Enter the new filter name and click the associated Create button. The Edit Filter screen appears.

Copy Filter

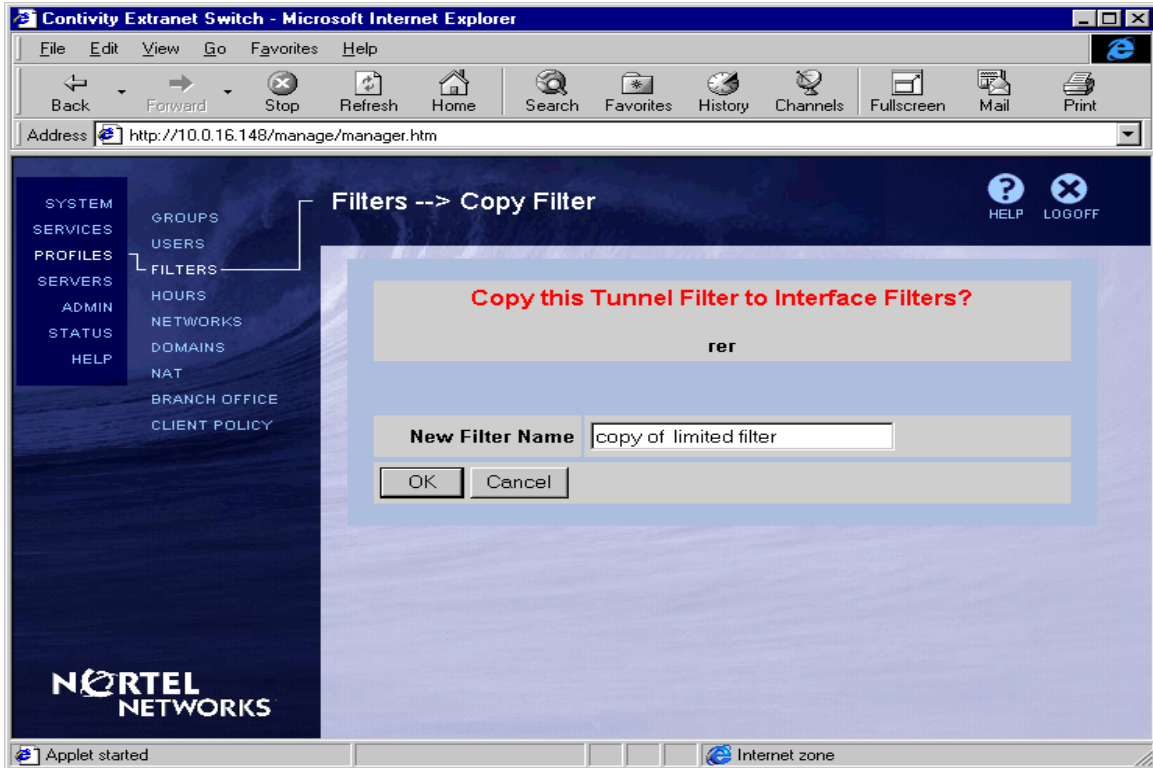
Use the Copy Filter buttons to copy an existing filter from one filter set to the other. For example, if you have already created a filter for tunnels, you can copy it for use by your Switch's interfaces.



Note: If you plan to use a filter for both tunnels and interfaces, it must appear in both windows on the Filters screen.

To copy a filter, click on the existing filter in one Current Filters window, then click the appropriate Up or Down button to move the filter to the other Current Filters window. The Copy Filters screen appears, asking you to confirm that you want to copy the filter.

Figure 102 Copy Filters



You can also rename the filter before you copy it.



Note: Additional set up steps might be required if you copy a tunnel filter for use by a Contivity Firewall. This is because the traffic that uses the Contivity Firewall traverses two of the Switch's interfaces (for example it might enter via a public interface and exit through a private interface). On the other hand, tunnel traffic only enters and exits through a single physical interface.

Edit Filter

This screen allows you to eAdd, Edit, Delete, or alter the ordering of Filter Rules by moving them up or down in the rules priority list. If you are editing a tunnel filter, you can also enable or disable HTTP, SNMP, FTP, Telnet, or PING through a tunnel as part of this filter.



Note: The Allow Management Traffic portion of this screen does not appear for Interface Filters.

Filter Set

The name of the filter that you are currently editing.

Rules in Set

Lists the rules that are already contained in the filter that you are editing.

<< *(Add Rule)*

Click on a rule from the Available Rules list on the right of the screen, then click on the left arrow to add the rule. This adds the selected rule to the current rules list. The new rule is added after the rule currently selected in the Rules in Set list.

>> *(Remove Rule)*

Click on a rule, then click the right arrow to remove or delete it from the Rules in Set list.

^ *(Move Up)*

Click on a rule in the Rules in Set list, then click the up arrow to move the rule up one place in the list.

∨ *(Move Down)*

Click on a rule in the Rules in Set list, then click the down arrow to move the rule down one place in the list.

Available Rules

This field lists all of the rules that are available on the Switch to add to the filter. They appear in the format of:

Name: Rule String (according to the Cisco format)

Manage Rules

Click to view the Current Rules screen, from which you can Create, Edit, Copy, or Delete a Rule.

Allow Management Traffic



Note: The Allow Management Traffic section applies only to tunnel filters, and does not appear on the screens for interface filters.

By manipulating these options, you can restrict management access to the Switch through tunnels. Each filter set has an explicit list of management services. By specifying the management services allowed through a tunnel, you can control which groups of users are able to perform different management tasks while tunneled into the Switch.

The Switch's default filter is Permit All, and the settings for this filter are to allow HTTP, SNMP, and PING. But if you create a new filter, all Management Traffic settings are disabled by default.

The management protocols are broken into two groups. The Local Services selections refer to services that reside on the Switch. The Remote Servers selections refer to services that reside on other systems that are used by the Switch. When enabled, network traffic for these services is allowed through tunnels.

The management services apply to user and branch office connections. These options do not affect HTTP, SNMP, FTP, Telnet, or PING protocol traffic that is passing through the Switch outside a tunnel.

For these Local Services

HTTP

Enable or disable access to the Web server on the Switch.

SNMP

Enable or disable SNMP “gets” to the Switch.

FTP

Enable or disable FTP “puts” or “gets” to the Switch.

Telnet

Enable or disable Telnet access to the Switch.

PING

Enable or disable PING access to the Switch.

RADIUS

Enable or disable access to the Switch’s RADIUS authentication service.

FIREWALL

Enable or disable Check Point FireWall-1 management traffic. When enabled, Check Point Management stations can communicate via a tunnel with the Switch’s integrated Check Point FireWall-1.

For these Remote Servers

The Remote Servers options restrict traffic to external services that are required by the Switch. By specifying these services, you can restrict which tunnels on a Switch can send protocol traffic for external services it requires.

FTP

Enable or disable FTP access from the Switch to external FTP servers on the other end of a tunnel. The FTP back-up and FTP upgrades facilities are examples of external services that are controlled by this option.

DHCP

Enable or disable access to dynamic host configuration protocol (DHCP) servers from the Switch.

RADIUS

Enable or disable the Switch's ability to access a remote RADIUS server.

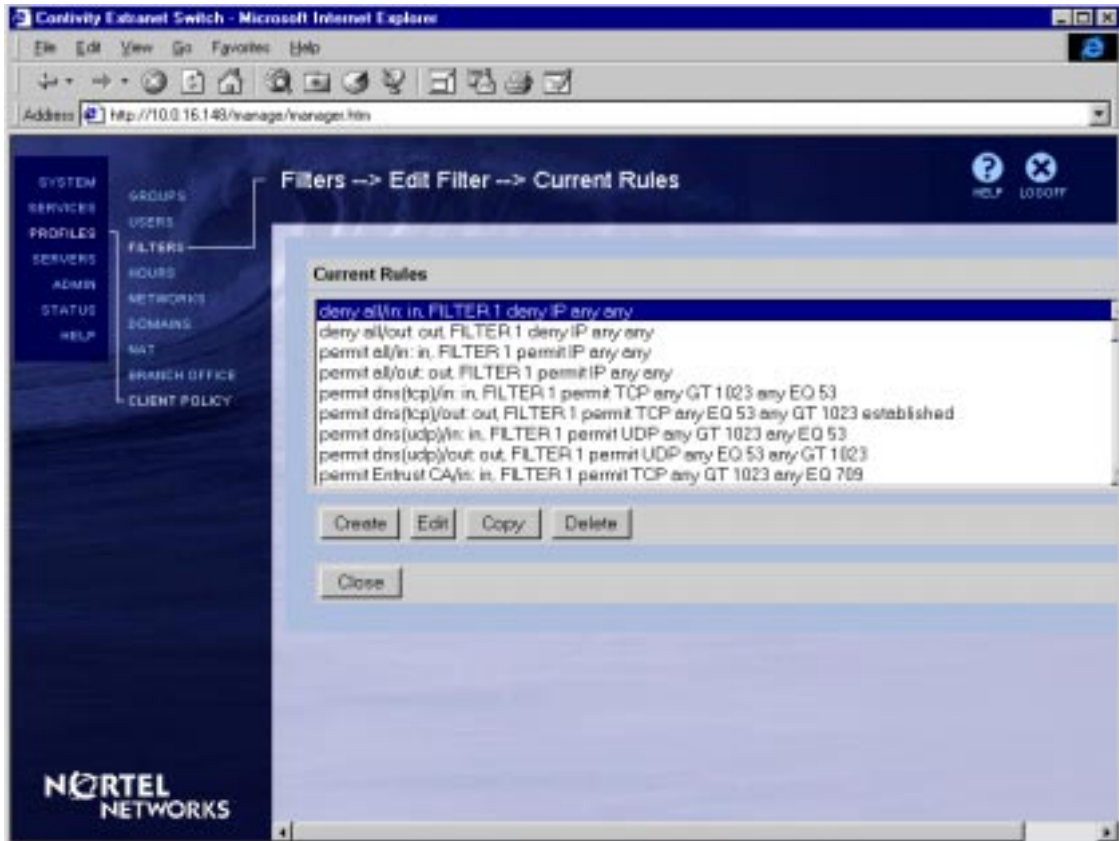
DNS

Enable or disable remote users from using the Domain Name Server (DNS) service for the Switch.

Manage Rules

Click Manage Rules to view the current rules that you can manage.

Figure 103 Manage Rules



Create

Click to create a new Rule. The Rule Definition screen appears.

Edit

Click on a rule then click Edit to modify it (refer to Edit Filter” for details).

Copy

Click on a rule then click copy to create a copy of the rule.

Delete

Click on a rule, then click Delete to remove it from the list of possible filter rules. You are prompted to confirm the rule deletion.

If the rule is contained in any filters, the deletion screen prompt informs you of how many filters are affected by the rule's deletion.

Creating, Editing, and Copying a Filters Rule

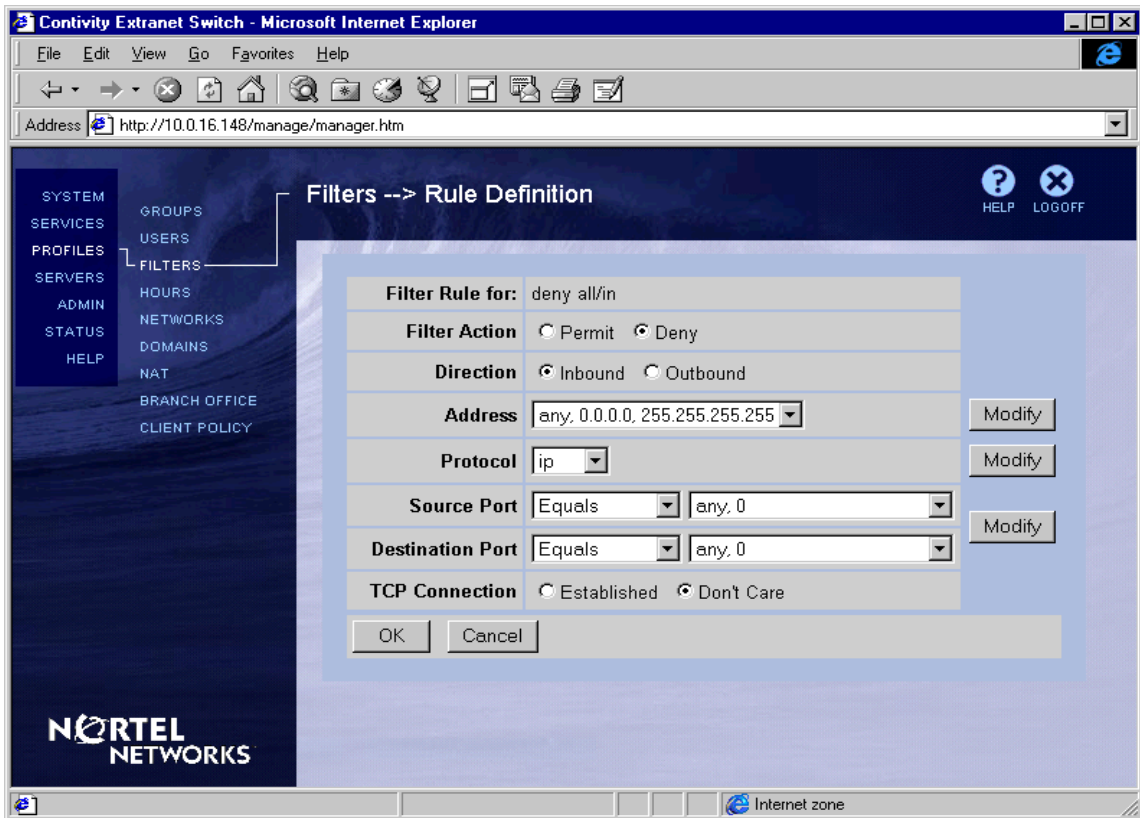
The Create Filter Rule Definition, the Edit Filter Rule Definition, and Copy Filter Rule Definition screens are similar and therefore the field descriptions are presented together in this section.

Figure 104 Create Filters Rule Definition

The screenshot shows a web browser window titled "Contivity Extranet Switch - Microsoft Internet Explorer" with the address bar displaying "http://10.0.16.148/manage/manager.htm". The main content area is titled "Filters --> Rule Definition" and contains a form for defining a filter rule. The form includes the following fields and options:

- Rule Name:** A text input field.
- Filter Action:** Radio buttons for ☒ Permit and ☐ Deny.
- Direction:** Radio buttons for ☒ Inbound and ☐ Outbound.
- Address:** A dropdown menu showing "any, 0.0.0.0, 255.255.255.255" and a "Modify" button.
- Protocol:** A dropdown menu showing "tcp" and a "Modify" button.
- Source Port:** A dropdown menu showing "Equals" and a text input field showing "any, 0", with a "Modify" button.
- Destination Port:** A dropdown menu showing "Equals" and a text input field showing "any, 0", with a "Modify" button.
- TCP Connection:** Radio buttons for ☐ Established and ☒ Don't Care.
- Buttons:** "OK" and "Cancel" buttons at the bottom of the form.

The sidebar menu on the left includes the following items: SYSTEM, SERVICES, PROFILES, FILTERS (highlighted), SERVERS, ADMIN, STATUS, HELP, GROUPS, USERS, FILTERS (sub-menu), HOURS, NETWORKS, DOMAINS, NAT, BRANCH OFFICE, and CLIENT POLICY. The Nortel Networks logo is visible in the bottom left corner of the sidebar.

Figure 105 Edit Filter Rule Definition

Rule Name or Filter Rule For:

Create a Rule Name or show the Rule that you intend to modify. The last rule of a filter by default is always Deny any packet. Therefore, build your filter groups by first permitting the services that you want to allow into or out of the Switch. Deny any packet does not appear in the rules list. For efficiency, you might want to add a Deny rule earlier in the rules sequence so that an unwanted packet is dropped before processing all rules in a filter.

Filter Action

The Filter Action determines the Switch's action when a packet matches the rule.

Permit

Click Permit to allow such packets.

Deny

Click Deny to drop such packets.

Direction

You can filter packets from either the Inbound or Outbound direction.

For tunnel filters, the direction setting is relative to the Switch. For example, if Outbound is selected, packets from the Switch headed in the Outbound direction would be filtered (into the tunnel, which is typically out to the Public network).

For interface filters, the direction setting is relative to the interface that the filter is applied to. For example, if Outbound is selected, and the interface filter is applied to a private interface, then packets heading out to the private network from the interface would be filtered.

Inbound

The filter is applied to Inbound packets. For tunnel filters, Inbound is from the Public Data Network (PDN) to the Private network. For interface filters, Inbound is traffic that is received by the interface.

Outbound

The filter is applied to Outbound packets. For tunnel filters, Outbound is from the Private network to the Public Data Network (PDN). For interface filters, Outbound is traffic that is transmitted by the interface.

Address

You can filter packets to or from a given Inbound or Outbound Address. Either select the existing address from the drop-down list box, or click Modify to create a new address and mask, or delete an existing address and mask. Refer to *Current Addresses*” for additional information.

The Address is always an enterprise (private) address: for inbound filters, it is a destination address; for outbound filters it is a source address. You might want to create a rule to permit traffic outbound to all addresses.

Protocol

- Click the drop-down list box to select the appropriate Protocol. To add, edit, or delete Protocols that you want to filter, click Modify. Refer to Current Protocols” for additional information. The default list follows:
- ICMP -- Internet Control Message Protocol is a Network protocol layer. The PING utility generates ICMP packets. PING is often used to see if a system’s network is available.
- IP -- Internet Protocol is a Network layer protocol in the TCP/IP stack that offers a connectionless internetwork service. IP packets that are encapsulated within other packets create “IP over IP.” Multicast IP packets (packets that have multicast destinations), carried between networks that support multicasting over intermediate networks that do not, are the most common implementation. Conferencing and other services that are offered through Multicast Backbone (MBONE) are examples.
- TCP -- Transmission Control Protocol is a transport layer protocol in the TCP /IP protocol stack. This is a connection-oriented protocol that provides reliable full-duplex data transmission. Web browsers using HTTP and FTP are examples.
- UDP -- User Datagram Protocol is a transport layer protocol in the UDP/IP protocol stack. UDP is a connectionless service that exchanges datagrams without acknowledgment or delivery guarantees, and therefore requires that error handling and retransmissions are handled by other protocols. DNS and WINS are examples.

Source and Destination Ports

You can filter packets to or from the Source and Destination Ports. This would permit or deny any packets from being transferred by the Switch based on the Source and Destination Ports. If the port matches any of the following variables, then the configured action is taken.

For example, if a packet's Source Port Equals that in the Filter rule, and the rule is to deny packets from that Source Port from entering the Switch, then the packet is dropped. The Source or Destination is relative to the direction of the rule.

- Equal
- Not equal
- Greater than
- Less than
- GT (greater than) or equal
- LT (less than) or equal

The most common Source and Destination Ports in use are available in an alphabetical drop-down list box. Select the appropriate port for your filter rule. To add, edit, or delete Ports that you want to filter, click Modify. Refer to “Create or Edit Port” for additional information.

TCP Connection

The TCP Connection setting is used only when the protocol is TCP. This can be useful when setting up rules if you need to identify whether the packet is initiating a TCP connection.

The TCP Connection establishment (ACK bit) allows you to configure a filter rule that does not permit internal systems to establish connections with tunneled hosts. It does, however, permit tunneled hosts to establish connections with internal servers. To configure this, permit TCP packets without the ACK bit (Don't Care) into the tunnels only and not out of the tunnels.

Established

Select Established to identify packets in an already established TCP Connection.

Don't Care

Select Don't Care when you do not care whether a TCP Connection has been established.

Common Filter Modify Fields

Under the Filters→Rules Definition screen, the Modify button for the Addresses, Protocols, and Ports screens all have common fields, which are listed here using the subject Addresses. Each of the other two filter fields responds as stated here, though of course the subject of the action is either Protocols or Ports.

The fields that are not common to other screens are described with the particular screen.

Create

Click to add a new Address.

Edit

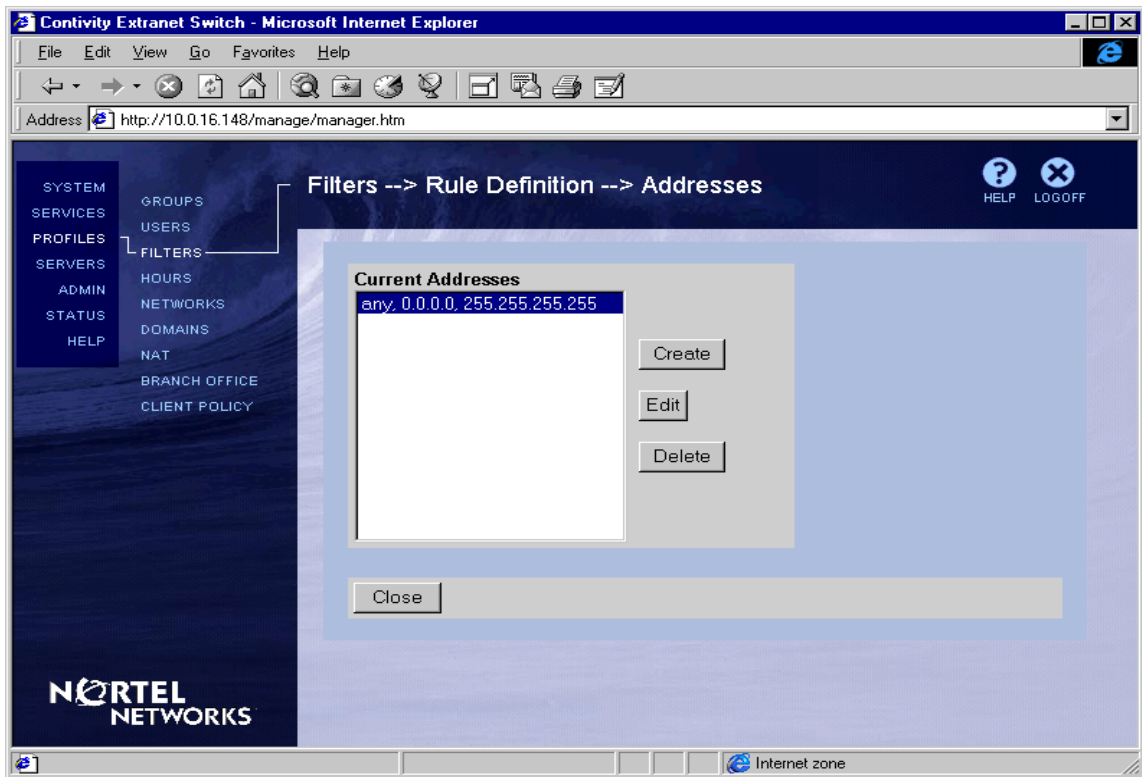
Click to Edit a selected Address Mask.

Delete

Click to Delete a selected Address.

Current Addresses

The Current Addresses appear in the screen. To edit or delete an Address, click the Address, then click Edit or Delete. To create an Address, click Create.

Figure 106 Current Addresses

Current Addresses

Displays the current IP addresses that are to be filtered.

Create or Edit Address

Following is a sample Create or Edit Address screen.

Figure 107 Create or Edit Addresses

The screenshot shows a web browser window titled "Contivity Extranet Switch - Microsoft Internet Explorer". The address bar displays "http://10.0.16.148/manage/manager.htm". The browser's menu bar includes File, Edit, View, Go, Favorites, and Help. The toolbar contains various navigation and utility icons. The main content area has a dark blue header with the text "Filters --> ... Addresses --> Create Address" and icons for HELP and LOGOFF. On the left, a vertical navigation menu lists: SYSTEM, SERVICES, PROFILES, SERVERS, ADMIN, STATUS, and HELP. A sub-menu for PROFILES is expanded, showing: GROUPS, USERS, FILTERS, HOURS, NETWORKS, DOMAINS, NAT, BRANCH OFFICE, and CLIENT POLICY. The "Create Address" form is centered and contains three input fields: "Address Name" (empty), "Address" (empty), and "Wildcard" (containing "0.0.0.0"). Below these fields are "OK" and "Cancel" buttons. The Nortel Networks logo is in the bottom left corner, and the "Internet zone" status is in the bottom right corner.

Address Name

Enter the IP Address Name for the entry to be created or edit an existing Address Name.

Address

Enter the IP Address for the entry to be created or edit an existing Address.

Wildcard

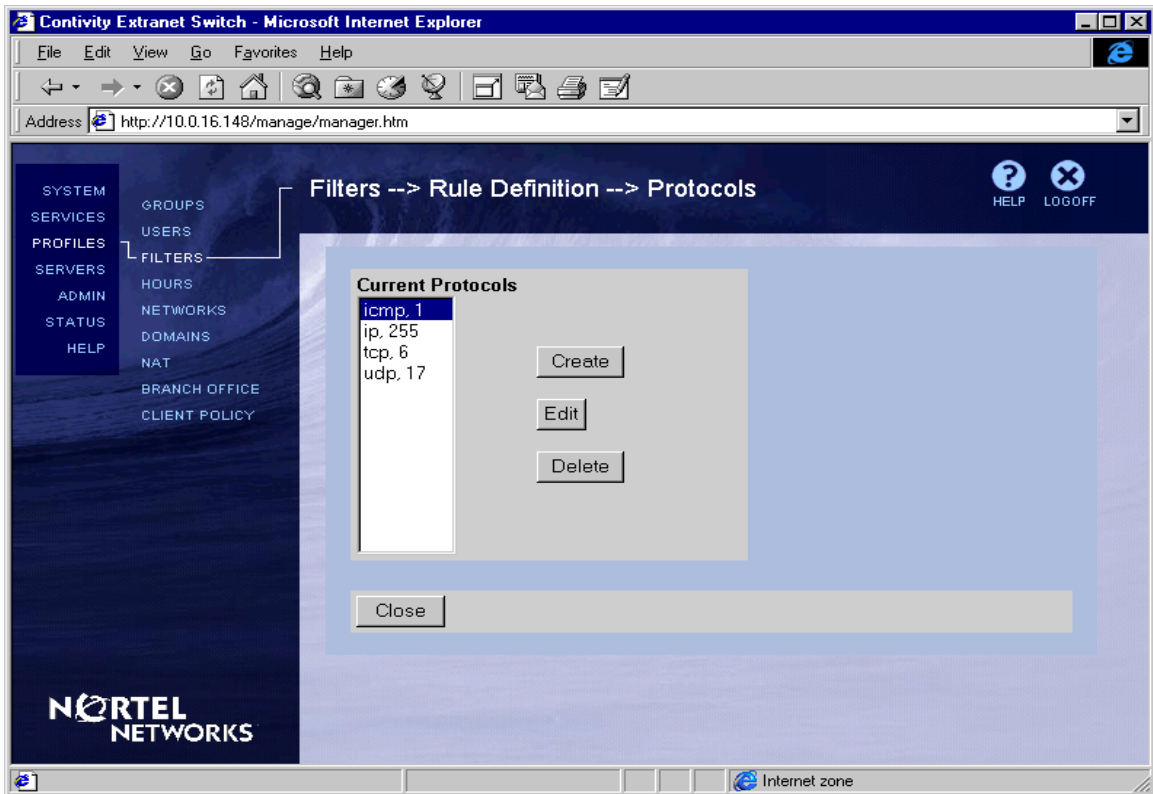
Enter the Wildcard to be applied to the address or edit an existing Wildcard. This follows the Cisco filter rule convention. Place ones in the bit positions that you want to ignore. Following are three Wildcard examples:

Table 22 Wildcard examples

255.255.255.255	The Address does not matter (any address).
0.0.0.0	The system looks for an exact Address match.
0.0.3.255	The first two octets and the six most significant bits of the third octet create the address match.

Current Protocols

The Current Protocols appear in the screen. To edit or delete a protocol, click the protocol number, then click Edit or Delete. To create a protocol, click Create.

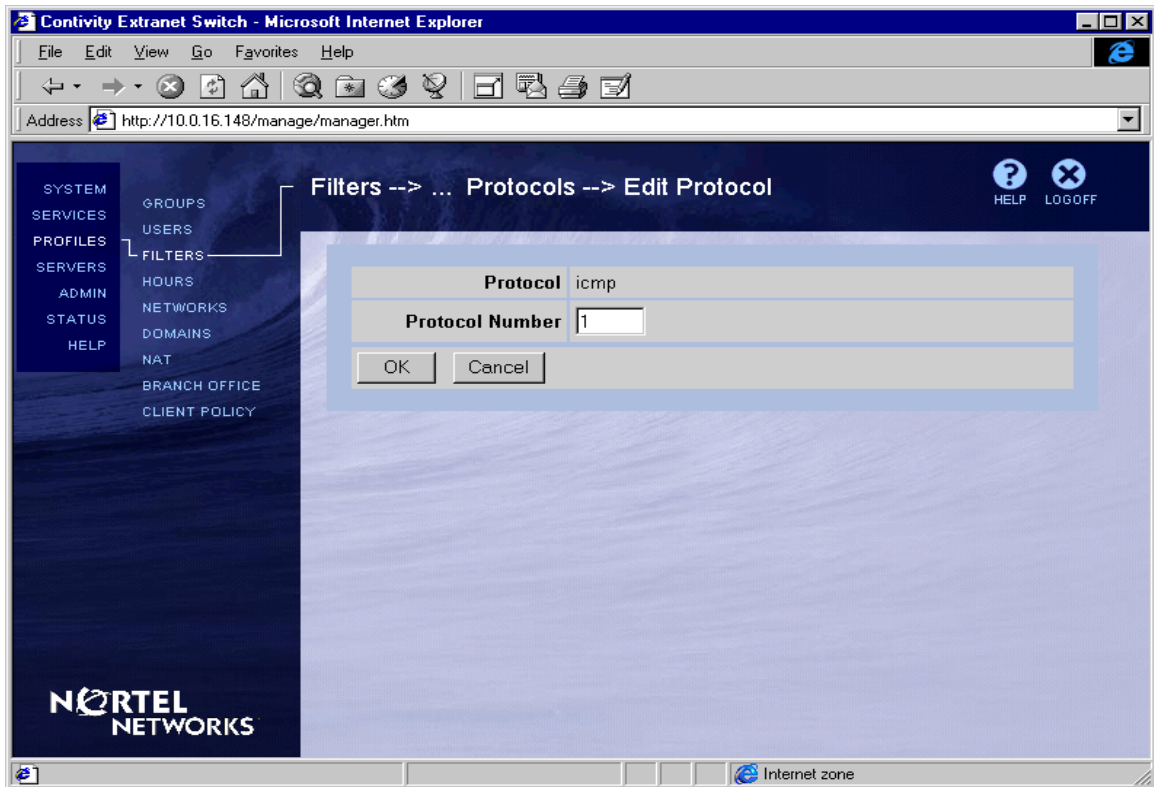
Figure 108 Current Protocols

Current Protocols

Lists the Protocols that are currently configured for this filter.

Create or Edit Protocol

Following is a sample Create or Edit Protocol screen.

Figure 109 Create or Edit Protocols

Protocol

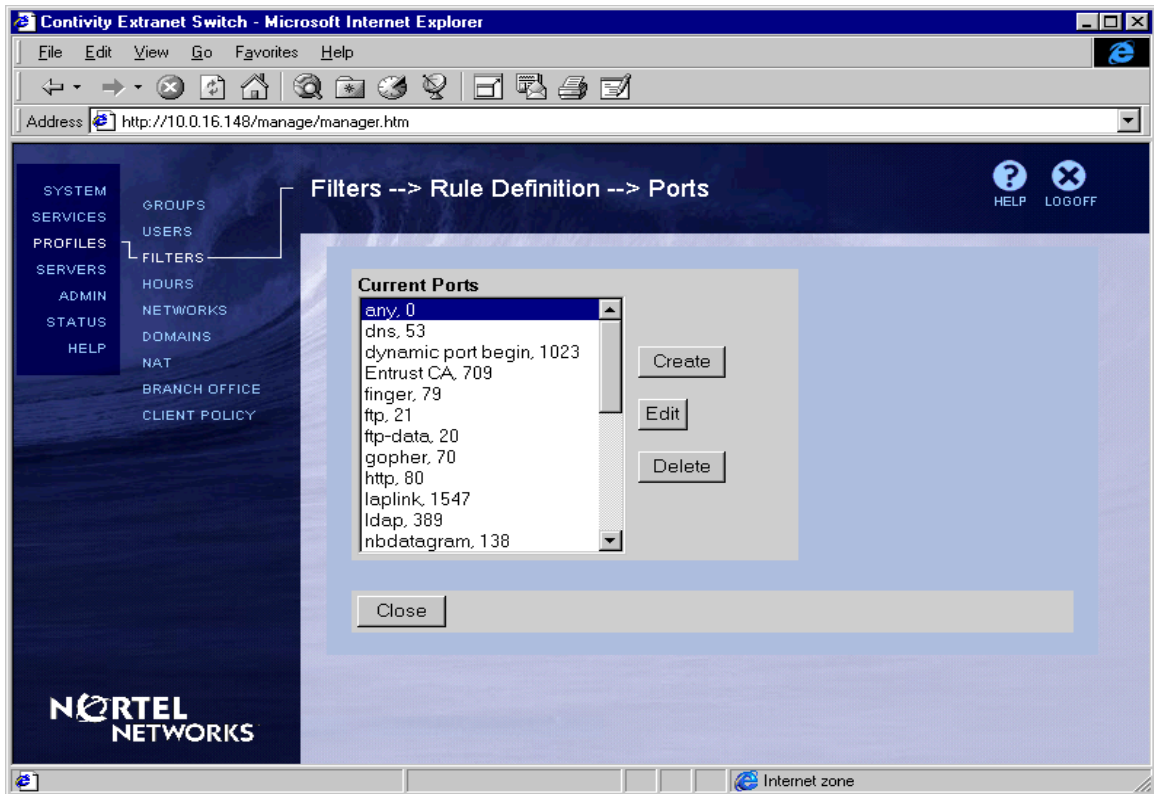
Enter a new or edit an existing Protocol Name.

Protocol Number

Enter a new or edit an existing Protocol Number.

Current Ports

The Current Ports appear in the screen. To edit or delete a port, click the port number, then click Edit or Delete. To create a port, click Create.

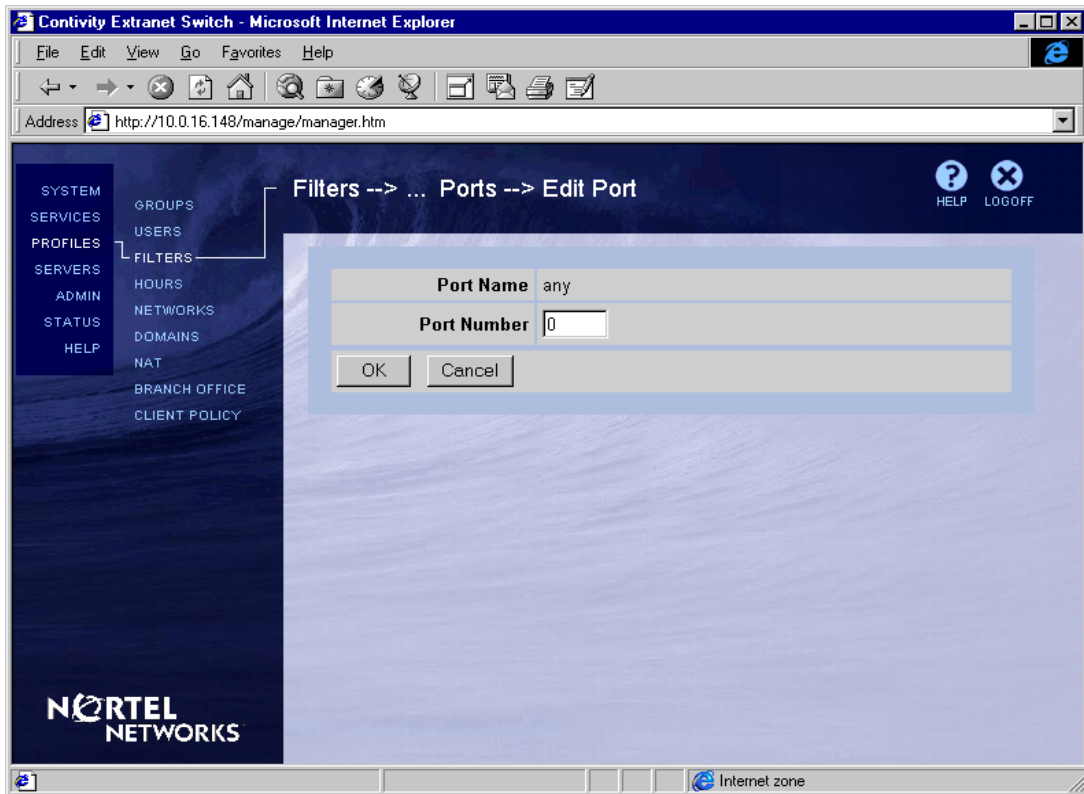
Figure 110 Current Ports

Current Ports

Lists all of the currently configured ports by name and number.

Create or Edit Port

Following is a sample Create or Edit Port screen.

Figure 111 Create or Edit Port

Port Name

Enter a new or edit an existing Port Name.

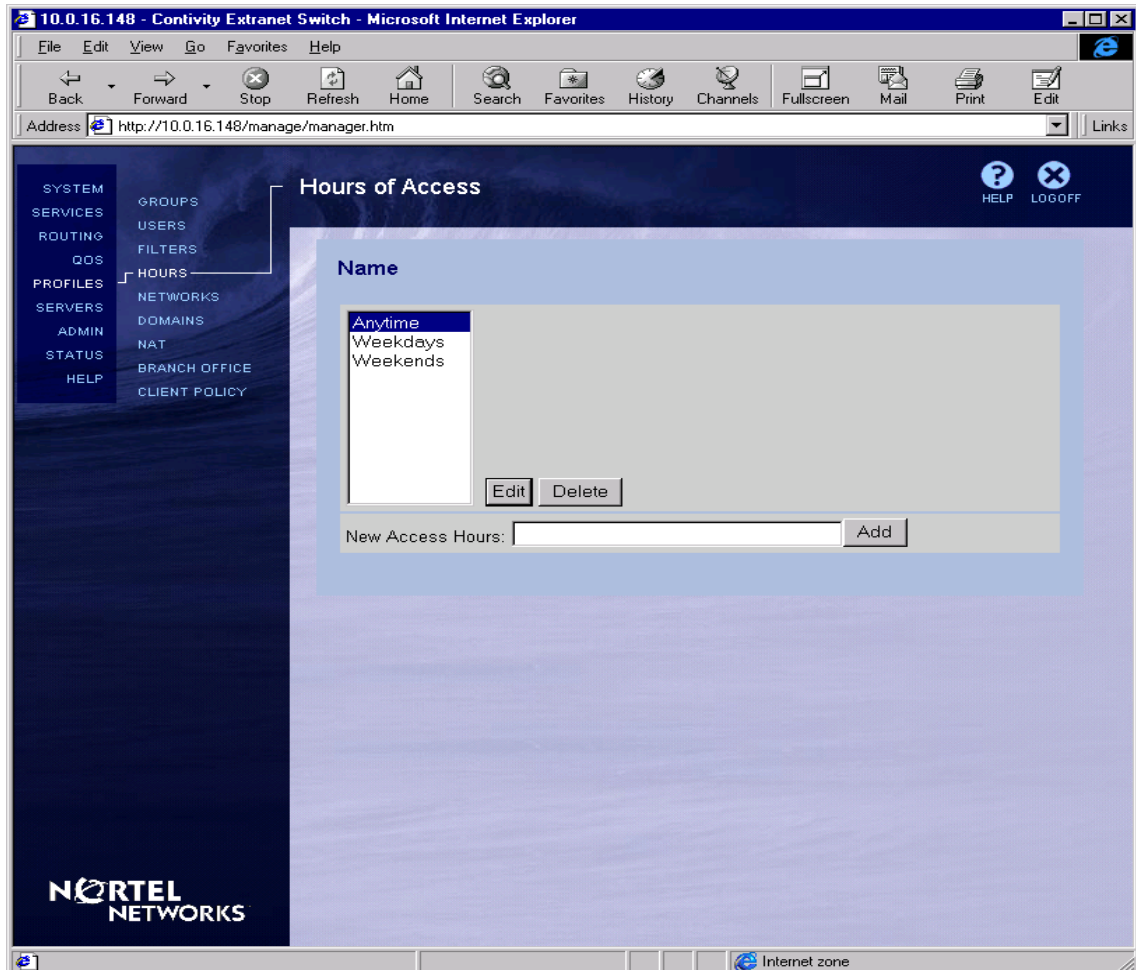
Port Number

Enter a new or edit an existing Port Number.

Hours

The Hours of Access screen allows you to set predetermined times during which you can permit a group of users extranet access. This time allocation provides for very specific access at certain hours only or complete access anytime; or variations that allow you to shut users out to perform network maintenance.

Figure 112 Hours of Access



Name

The Name of the defined schedules that can be assigned to Groups appear in the list box. Use one of the available buttons to modify the list. Default is **Anytime**.

Edit

Click to modify the profile of the access schedule currently selected.

Delete

Click to Delete the access schedule currently selected. You cannot delete a particular schedule of hours if it is being used by a group.

New Access Hours

Enter the Name for a new profile of access hours.

Add

Click to Add an access profile to the list of defined schedules.

Edit Hours of Access

This screen allows you to configure exact times that a group is permitted access to the Switch. The ranges are Monday to Sunday, 00:00:00 to 23:59:59, based on a 24-hour clock.

Figure 113 Edit Hours of Access

10.0.16.148 - Contivity Extranet Switch - Microsoft Internet Explorer

File Edit View Go Favorites Help

Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail Print Edit

Address <http://10.0.16.148/manage/manager.htm> Links

SYSTEM
SERVICES
ROUTING
QOS
PROFILES
SERVERS
ADMIN
STATUS
HELP

GROUPS
USERS
FILTERS
HOURS
NETWORKS
DOMAINS
NAT
BRANCH OFFICE
CLIENT POLICY

Hours of Access --> Edit

HELP LOGOFF

Name: Anytime

Day	Hours Allowed 24 Hour time format (hh:mm:ss)
☒ Monday	00:00:00 to 23:59:59
☒ Tuesday	00:00:00 to 23:59:59
☒ Wednesday	00:00:00 to 23:59:59
☒ Thursday	00:00:00 to 23:59:59
☒ Friday	00:00:00 to 23:59:59
☒ Saturday	00:00:00 to 23:59:59
☒ Sunday	00:00:00 to 23:59:59

OK Cancel

NORTEL NETWORKS

Internet zone

Day

Click the Days of the week that you want this group to have access to the Switch, from Monday to Sunday.

Hours Allowed

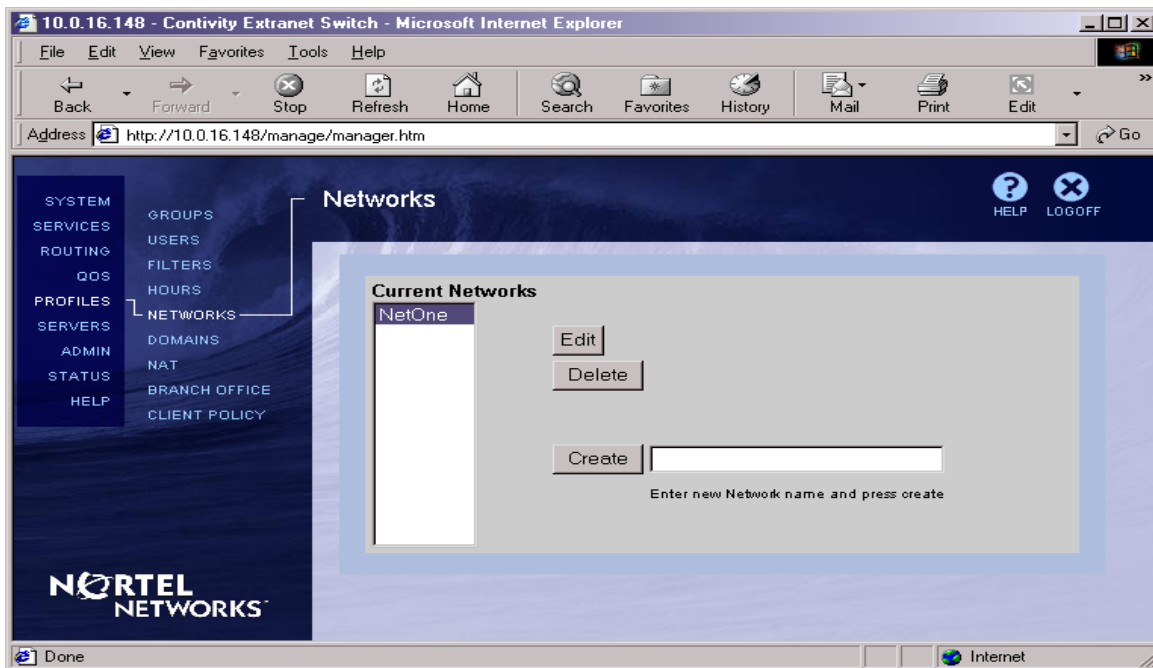
Enter the Hours Allowed that you want this group to have access to the Switch: from 00:00:00 to 23:59:59, based on a 24-hour clock.

Networks

The Networks screen allows you to specify network routes that are tunneled when you enable the split tunneling or branch office features.

After you specify networks, you associate them to specific groups for tunneling capabilities through the Profiles→Groups→Connectivity Edit screen. You specify branch office networks through the Profiles→Branch Office Edit screen.

Figure 114 Networks



Current Networks

Shows the currently configured network routes that you can select when specifying split tunneling or branch offices.



Note: A maximum of 16 routes are allowed on the August 1995 version of Windows 95 systems; the Switch displays more than 16 routes, but you cannot tunnel through them.

Edit

Click the Network that you want to modify, then click the Edit button. The Filter Rules for that group appear.

Delete

Click to Delete a Network that you no longer intend to use. The name is removed from the list. You cannot delete a Network that is being used.

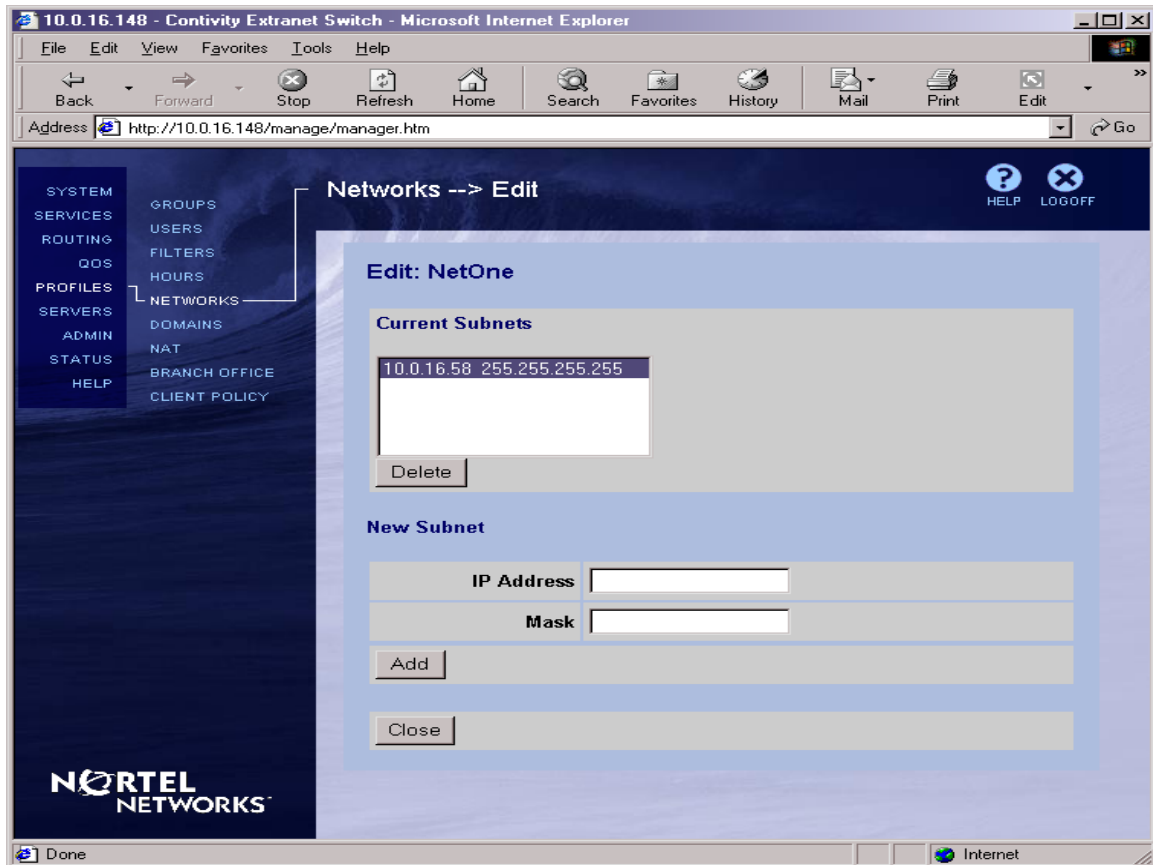
Create

Enter the new network name and click to Create a new network; the Networks Edit screen appears.

Networks Edit screen

The Networks Edit screen allows you to assign IP addresses and subnet masks to the networks.

Figure 115 Networks Edit



Current Subnets For

Shows the currently configured IP addresses and subnet masks for the network that you are editing.

New Subnets For

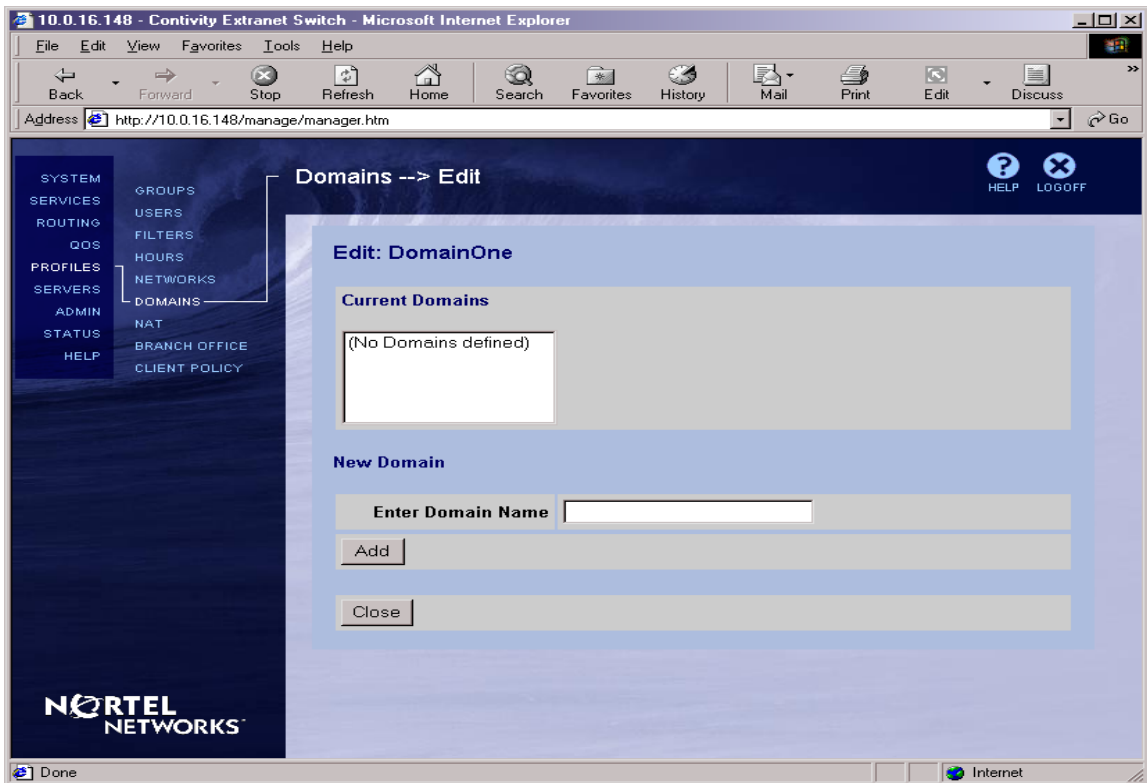
Enter the IP Addresses and Subnet Masks for the networks, then click Add.

Domains

The Domains screen allows you to specify the domains that are used by the Client Auto Connect feature. This screen helps simplify management by grouping domains into sets. You then specify which sets of domains are used for particular IPSec tunnels on the Profiles→Groups→Edit IPSec screen.

When a remote client user attempts to connect to a location, such as a web site, that is in a specified domain or set of domains, the Client Auto Connect feature is started. For more information, refer to Forced Logoff.”

Figure 116 Domain



Current Domain Sets

Shows the currently configured sets of domains that you can use when specifying the Client Auto Connect feature.

Edit

Click the domain set that you want to modify, then click the Edit button. The Edit Domain Set screen appears.

Delete

Click to delete a domain set that you no longer intend to use. The name is removed from the list. You cannot delete a domain set that is currently being used.

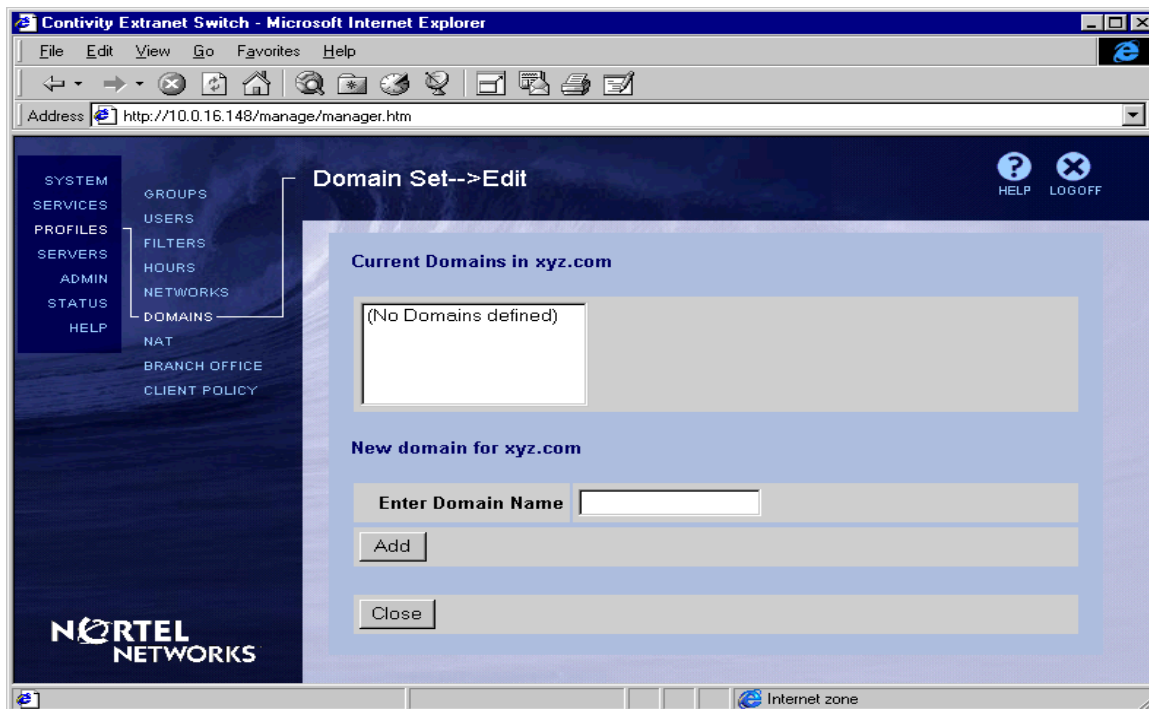
Create Domain

Enter the name of the new domain set, then click the Create Domain button. The new name is added to the Current Domain Sets field. You can then edit the domain set and add the names of the domains that you want included in the set.

Edit Domains screen

The Edit Domains screen allows you to add domains to the selected domain set.

Figure 117 Edit Domains



Current Domains in domain_set

Shows the name of the domain set that you are editing and the names of the domains that are in the domain set.

Delete

Select the domain you want to delete, then click the Delete button. The name is removed from the list. You cannot delete a domain from a domain set that is currently being used.

New Domain for domain_set

Enter the name of the domain you want to add to the domain set, then click Add. The new domain appears in the Current Domains in *domain_set* field.

Network Address Translation (NAT)

Network Address Translation (NAT) is the translation of one network IP address that is used within a LAN to a different IP address that is used outside the LAN. This feature allows a system to be identified by one address on its own network, yet be identified by a totally different address to systems on a different network.

Creating NAT Sets

NAT sets are collections of rules that make up a named set. You can create specific NAT sets for certain conditions, and assign the sets as they are appropriate to the conditions. NAT sets are typically applied to branch offices that use either static or dynamic address schemes.

The NAT screen allows you to create NAT sets and edit or delete any currently defined NAT sets. To create new NAT sets, you define a name and click Create.

When you edit an existing NAT set, the NAT Rules screen appears. The NAT Rules screen allows you to add new rules or edit existing rules. This screen lists the currently defined rules for a given set.

Translation Type

Select one of the following (refer to Translation Types for descriptions):

- Static
- Port
- Pooled

Internal

Enter the start and end addresses that represent the address pool that is used within the intranet.

Start Address

Enter the first available address that is used within the intranet address pool.

End Address

Enter the last available address that is used within the intranet address pool.

External

The External address is for the endpoint device. Enter the start and end addresses that represent the addresses used for the public network (Internet).

Start Address

Enter the first available address that is used for the public network.

End Address

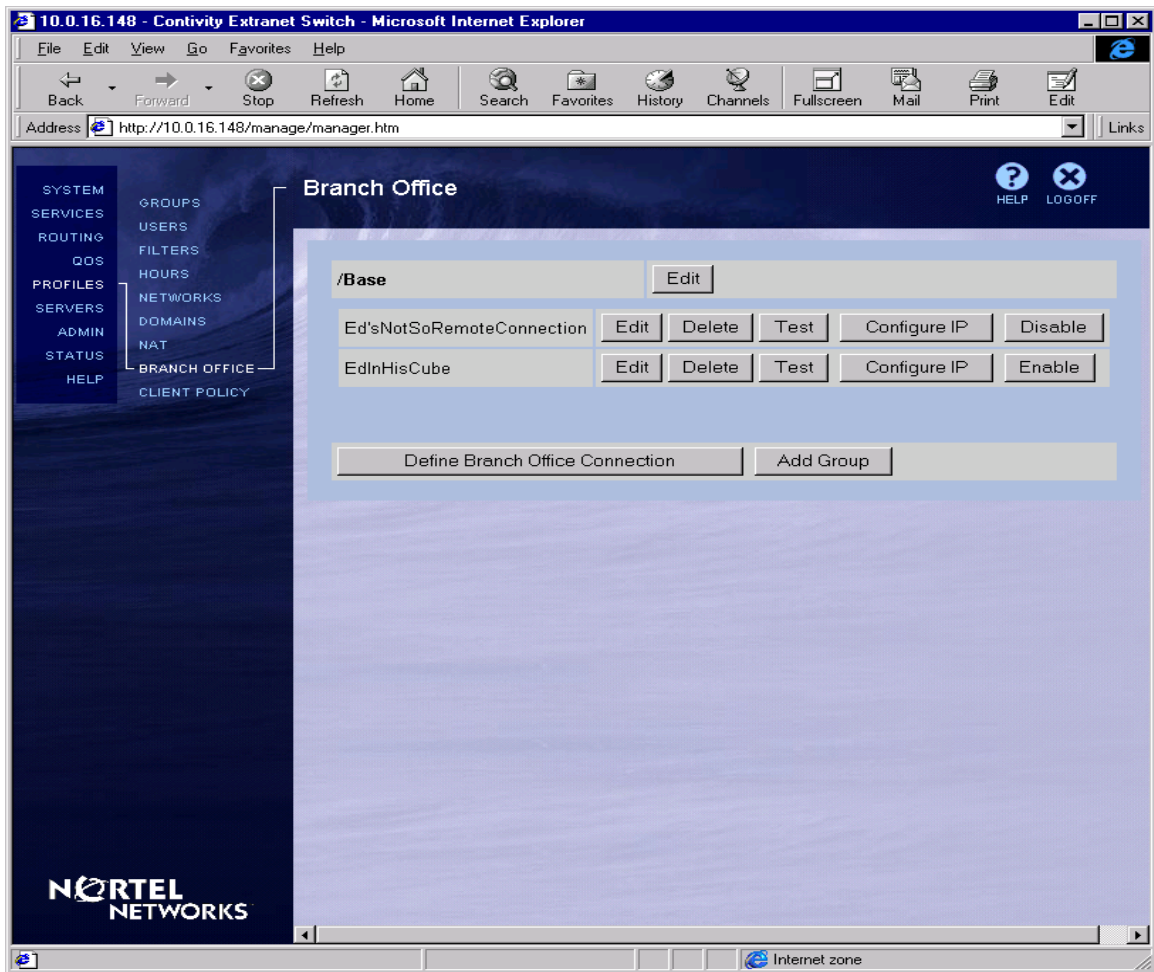
Enter the last available address that is used for the public network.

Branch Office

You access the Branch Office screen through the Profiles→Branch Office menu selection. You use the subsequent configuration pages to set up a branch office connection. They enable you to specify the attributes of the Switches that are participating in the connection and to set up network parameters, such as addresses and tunnel type, for the connection.

When you create a branch office connection, you associate it with a group. The branch office connection then inherits the attributes of that group. You can associate multiple branch offices with the same group, thereby saving set up time and increasing management efficiency. For example, you might plan on creating several VPN connections from various remote sales offices into your enterprise headquarters. In this case you would create all of the connections in the same group so they would all have the same attributes, such as hours of access, encryption method, and password management.

You use the main Branch Office screen to create new branch office connections and to edit or delete existing connections. The screen also enables you to add or edit the group that is associated with your branch office connection.

Figure 118 Branch Office

Edit

Accesses the Edit screen for either the selected group or the selected branch office connection.

Delete

Deletes the selected group or branch office connection.

Test

The Test button provides a mechanism for you to verify that the branch office connection is properly configured and that the remote gateway remains reachable. Detailed messages are sent to the Event Log to help identify failure events.

When you click the Test button, establishment of the Branch Office tunnel is attempted. If the test is successful, this insures that the remote and local gateway configuration is correct. If for any number of reasons the connection establishment fails, a failure message should indicate what the configuration problem might be. The Event Log is used extensively during this test to provide details about the test. Additional logging is done as part of the tunnel protocols (L2TP and IPSec), which should provide enough information to determine the problem.

In some cases, however, the actual reason for the failure is due to some remote configuration issue that is not provided in failure exchange with the remote gateway. In such cases, it may be difficult for you to determine the exact reason. If possible, initiating the test from the remote gateway could provide the necessary details.

Configure IP

The Configure IP button accesses the Branch Office→Edit→IP screen. You use this screen to enable and disable a branch office and to configure routing for the branch office.

Enable/Disable

The Enable/Disable button toggles the Branch Office connection between states.

Define Branch Office Connection

The Define Branch Office Connection button accesses the Define Connection screen, which you use to name a new branch office connection and to associate it with a group.

Add Group Button

Accesses the Add Group screen, which is used to create a new group. The new group can then be associated with a branch office connection.

Add Group screen

This screen is used to add a new group that is associated with the branch office connection. The new group inherits the attributes (for example, Access Hours) of its parent group, which are then used by the branch office connection.

Parent Group

The drop-down list box shows all the branch office groups that have been set up on the Switch. Select the group whose attributes are inherited by the new group. Refer to the Profiles→Groups→Edit→Connectivity screen for additional details on the hierarchical structure of group attributes.

Group Name

The Group Name identifies the new group that are associated with the branch office connection. The Group Name can be a maximum of 64 characters (spaces are permitted).

Edit Group

The Edit Group screen is accessed either through the Edit button on the Branch Office screen or through Profiles→Groups: Edit screen. This screen is used to set up Connectivity, IPSec (for IPSec tunnels), and routing attributes for a particular group. Edit the configuration parameters as appropriate.

Refer to Profiles→Groups: Edit for configuration details. The Branch Office configuration requires only a subset of the options that are described in those sections.

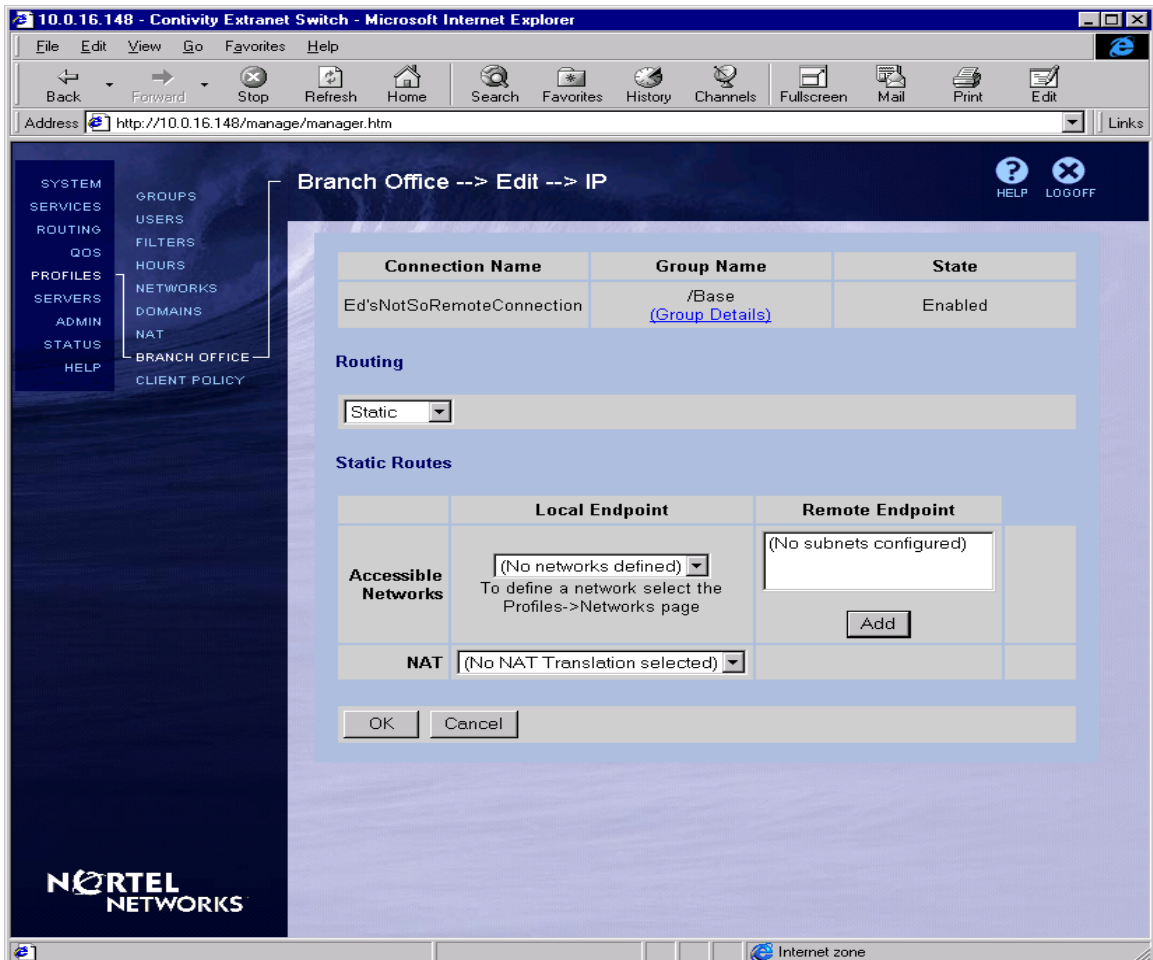
The Idle Timeout setting is valid for traffic coming into the device only.



Note: Branch Office connections do not support the CA Certificate Allow All feature. Therefore, you must have an explicit entry for each Branch Office connection. Only branch offices with the branch office's certificate subject distinguished names entered into the Profiles→Branch Office: Define Branch Office Connection screen can authenticate using certificates issued by the CA.

Configure IP

The Configure IP button accesses the Branch Office→Edit→IP screen. You use this screen to enable and disable a branch office and to configure routing for the branch office.

Figure 119 Branch Office→Edit→IP

Connection Information

Connection Name

Displays the name of this branch office connection.

Group Name

The Group Name list contains the names of all groups that have been set up on this Switch. Select the group that you want to use for the branch office connection. The group is a child of its associated Parent Group and inherits the Parent Group's network access attributes (refer to the Profiles→Groups→Edit→Connectivity screen for details). You can later modify the new group's inherited options.

State

Shows the current state of this branch office connection, either enabled or disabled.

Routing

Use the drop-down list box to select either Static or Dynamic routing for this branch office connection.

Static Routes

Accessible Networks

You use the Accessible Networks section of the Static Routes to define local and remote networks to which the branch office has access. Use Profiles→Networks to define local networks and the Add button to define remote networks.

NAT

Use the drop-down list box to select from available NAT sets.

OSPF

OSPF State

Use this to enable and disable OSPF routing for the branch office.

Area ID

Area IDs are used as representations of parts of the OSPF network. They help to manage large numbers of networks so that they can exchange information within an area. If the area represents a subnet, the IP network number can be used for the Area ID. Each Area ID must be unique for OSPF. By default all Switches have an area named 0.0.0.0.

Cost

Enter a Cost value for OSPF routing.

RIP

Use this to enable and disable RIP for the branch office.

Define Branch Office Connection

The Define Connection screen is used to create a new branch office connection. To define a new connection, you first enter its name, then associate the new connection with a group. The connection inherits the attributes of that group. When you click OK, the branch office connection is created and the Define/Edit Connection screen appears.

Figure 120 Define Connection

Branch Office --> Define Connection

Connection Name	
Group Name	/Base
Control Tunnel	☐

OK Cancel

Connection Name

The name of the new branch office connection. The name can be a maximum of 64 characters (spaces are permitted).

Group Name

The drop-down list box contains the names of all groups that have been set up on this Switch. Select the group that you want to use for the branch office connection. The group is a child of its associated Parent Group and inherits the Parent Group's network access attributes (refer to the Profiles→Groups→Edit→Connectivity screen for details). You can later modify the new group's inherited options.

Control Tunnel

Put a check in the Control Tunnel check box to specify that this branch office connection is for a control tunnel. If you want a branch office connection to be a control tunnel, it must be configured as such at its initial configuration. When you create and save a branch office connection, you cannot later change the control tunnel specification for that connection. You must set up a new connection and create it as a control tunnel.



Note: Administrator User IDs are not tied to control tunnel IDs.

Define Connection/Edit Connection

The Define Connection and the Edit Connection screens allow you to Enable the Branch Office feature and to specify routing and networking information, local and remote identification, and authentication attributes for the branch office connection.

Connection Information

Connection Name

The name you assign to this branch office connection. The name can be a maximum of 64 characters (spaces are permitted).

Group Name

The group that defines the attributes that are used by the branch office connection. This group is a child (subset) of its associated Parent Group and inherits the settings from the Parent Group. You can click on the Group Details link to view or modify a subset of the group's settings. Modifications of a child group do not change the settings of the Parent Group.

State

Use the drop-down list box to toggle the state between enabled and disabled.

Configure Routing

Click the IP button to specify the type of routing to use for traffic going through the branch office connection.

- If you choose Static routing, you must manually specify the Accessible Networks (the private internal networks behind a Switch that can be accessed via the branch office connection).
- If you choose RIP, the routing protocol automatically determines the accessible networks based on information that is entered on the System→LAN Interfaces→Edit IP Address screen.

Click the drop-down list to choose the routing type that to be used for your branch office connection.

Configuration

Enable Branch Office Connection

Click to Enable the Branch Office feature for this Switch.



Note: As a security mechanism, the Enable Branch Office Connection selection is automatically disabled (the check mark is removed) when you attempt to save an incorrect configuration. For example, if you check the box to enable the branch office connection, then fail to specify the remote address, the Enabled check box is cleared (disabled) and an error message appears when you select the OK button to save your configuration.

Address

Used to specify the public interface IP addresses of the Switches that form the branch office connection. The Local Endpoint address is the public interface IP address of the Switch whose Management Interface you are using. The Remote Endpoint address is the public interface IP address of the Switch that forms the opposite end of the branch office connection.

Accessible Networks

If you have chosen the Static routing type, this field appears on the screen. It does not appear if you are using RIP routing. The accessible networks are the private internal networks that can be reached through the tunnel connections of this branch office connection.

- To specify the Local Endpoint networks, click the drop-down list to display a list of available local networks. These networks have been previously set up on the Profiles→Networks screen. The Local networks are the subnetworks on the private internal network of the local Switch (the Switch whose Management Interface you are currently using).
- To specify the Remote Endpoint networks, click Add to go to the Add Networks screen and add the remote networks for the branch office configuration. The Remote networks are the subnetworks on the private network of the remote Switch.

NAT

If you choose the Static routing type, this field appears on the screen. It does not appear if you are using RIP routing. Network Address Translation (NAT) allows a system to be identified by one address on its own network, and by a totally different address to systems on a different network. NAT enables you to build your extranet without requiring that you reconfigure or rename your existing network. NAT sets are defined on the Profiles→NAT screen. Refer to Network Address Translation (NAT)” for more information on NAT.

Click the drop-down list and select the NAT set that you want to use.

Filters

Select the desired filter that is associated with this connection, or use the default filters of permit all. Packet filtering controls the types of access allowed for users of this branch connection. Filters are based on various parameters, including Protocol ID, Direction, IP addresses, Source, Port, and TCP Connection Establishment. Filters are defined on the Profiles→Filters screen.

Click the drop-down list and choose the filter that you want this branch office connection to use. The default is permit all. You can specify one filter.

Tunnel Type

Use the drop-down list to change the tunnel type for the connection. The default type is IPSec. Click the drop-down list and select either IPSec, PPTP, or L2TP.



Note: If you change the Tunnel Type, the fields in the Authentication portion of this screen change to reflect the different configuration requirements for the new Tunnel Type.

Authentication

This portion of the screen allows you to configure the authentication that is used between the local and remote branch office Switches. The fields that appear in this screen depend on whether you are using an IPSec, PPTP, or L2TP tunnel type.

IPSec Authentication

Pre-Shared Key: Text or Hex String

This is an alphanumeric text or hexadecimal string that is used between the local and remote branches for authentication. In order for authentication to occur, you must use the same pre-shared string on both the local and remote branch offices.

Certificates

Certificates are associated with each endpoint gateway and allow for mutual authentication between two connections. The certificate portion of the screen includes information about the remote branch office system, the authority that issued the certificate, and the certificate identification.

Remote Identity

This is the name of the remote peer initiating the tunnel connection. You can use either a Subject Distinguished Name (Subject DN) or a Subject Alternative Name to uniquely identify the remote branch office system. Specifying both a full subject DN and a subject alternative name on this screen allows the remote peer to use either identity form when making a connection.

Valid Issuer Certificate Authority

Select a Valid Issuer Certificate Authority from the drop-down list box. This CA is the issuer of the remote peer's certificate or a higher level CA in the remote peer's certificate hierarchy. The CA must have the trusted flag set via the certificates screen. If a CA hierarchy is being used, all intermediary CAs below the trusted CA must have been imported to the Switch. These Certificate Authorities are configured from the System→Certificates: Generate Certificate Request screen.

Subject Distinguished Name

If you are using a distinguished name to identify the remote branch office site, you can choose to enter the DN as either a relative distinguished name or a full distinguished name. The DN entered here must exactly match the DN in the remote peer's certificate.

Relative

The Relative distinguished name has the following supported components:



Note: Do not include the attribute type as part of your entries in the Relative section. For example, for a name of CN=MySwitch, your entry would be MySwitch (without the CN attribute type).

- Common Name -- Enter the Common Name with which the server is associated.
- Org Unit -- Enter the Organizational Unit with which the server is associated.
- Organization -- Enter the Organization with which the server is associated.
- Locality -- Enter the Locality in which the server resides.
- State/Province -- Enter the State or Province in which the server resides.
- Country -- Enter the Country in which the user resides.

Full

You can directly enter the Full Distinguished Name (FDN) in this field rather than entering the individual components in the previously described Relative distinguished name fields. For example:

CN=MySwitch, O=MyCompany, C=US

Subject Alternative Name

You can optionally use a Subject Alternative Name in place of a Subject DN, and specify the format of the name. The following formats are acceptable.

- Email Name (for example, net_admin@company.com)
- DNS Name (for example, gateway.cleveland.company.com)
- IP Address (for example, 192.168.34.21)

Local Identity

The Local Identity is the name your Switch that you want to use to identify itself when initiating or responding to a connection request. You can use either a Subject Distinguished Name (Subject DN) or a Subject Alternative Name to uniquely identify your system. If you select a subject alternative name from your Switch's certificate, then that identity is used in place of your Switch's subject DN when communicating with peers.



Note: Your Switch's server certificate only has subject alternative names if your CA issued the certificate with the alternative names. For example, with the Entrust PKI the VPN connector can issue certificates with DNS names, IP addresses, or Email alternative names.

Server Certificate

Click the drop-down list box to view all certificates that have been issued to the server. Server Certificates are configured from the System→Certificates: Generate Certificate Request screen.

PPTP Authentication and L2TP Authentication

Authentication Type

Click the drop-down list and select the authentication method that you want to use for the branch office connection. Refer to “Common Tunnel Settings” for descriptions of the available authentication methods.



Note: When you change the Authentication Type, the screen immediately changes to reflect the requirements of the new authentication method. Any changes that you might have made on the Authentication part of the previous screen are lost.

Local UID

The user ID of the local Switch that you are configuring.

Peer UID

The user ID of the remote Switch that you are configuring.

Password

Enter the password for the UID, then confirm the password to verify that you entered it correctly. If you selected a variation of MS-CHAP V2 authentication, no password is required for the Local UID.

Details

Compression

Click to Enable or Disable compression. Refer to “Compression” for a detailed description of compression.

Compression/Encryption Stateless Mode

Click to Enable or Disable this selection. This selection is not used if encryption and compression are both disabled.

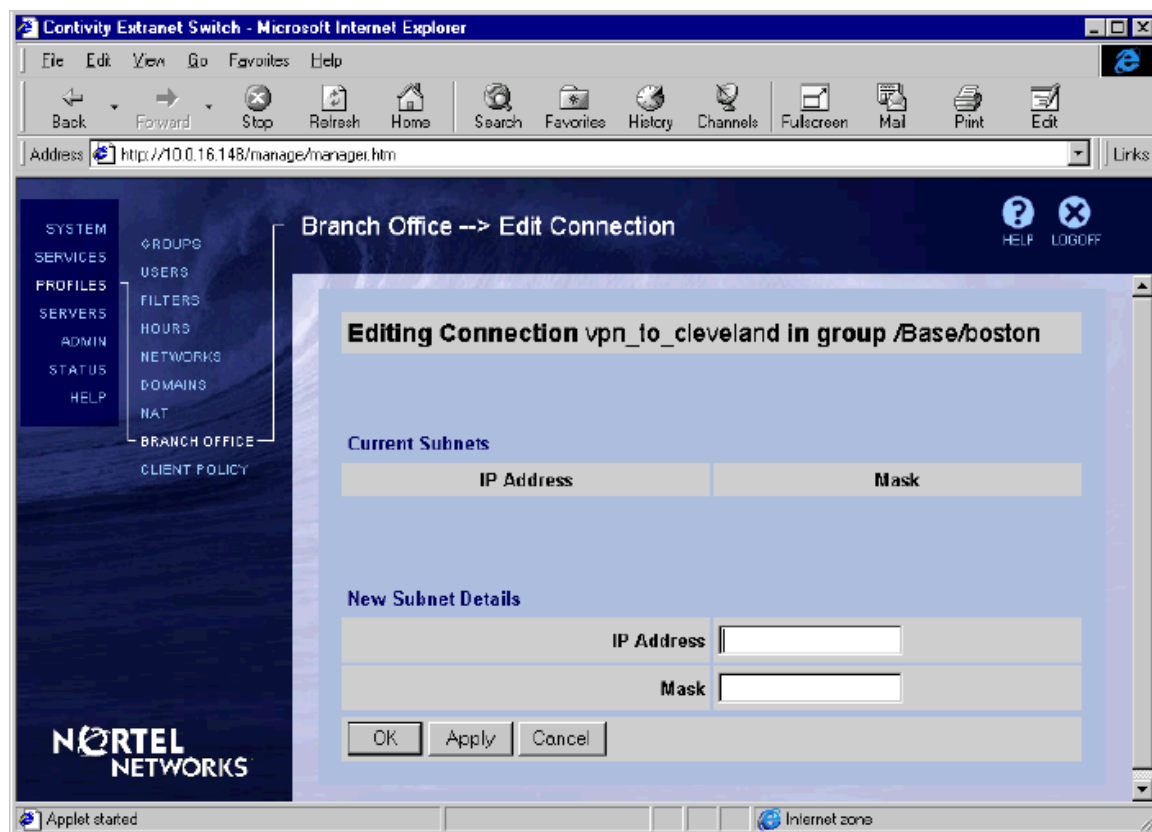
L2TP Access Concentrator (for L2TP Authentication only)

This field appears if you have selected L2TP as the preferred tunnel type for the branch office connection. Use this entry to specify the L2TP Access Concentrator that you want to perform authentication between the Switch and the NAS.

Add Remote Networks

When you click Add in the Accessible Networks section of the Edit Connection screen, the Add Remote Network screen appears.

Enter the IP address and subnet mask for the new remote network you want to add for the branch office connection.

Figure 121 Add Remote Networks

Client Policy

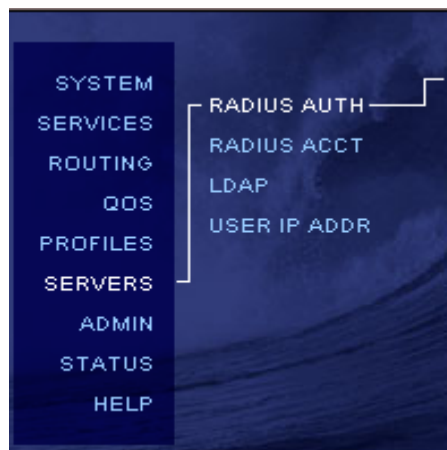
Client Policy helps prevent potential security violations that could occur when you are using the split tunneling feature. Split tunneling allows client data to travel either through a tunnel to the enterprise network or directly to the Internet. Although a powerful feature, this could allow an application on the client to maliciously forward packets from the Internet to the enterprise network.

Chapter 6

Servers

This section provides information about authentication servers for users who are tunneling into the Switch.

Figure 122 Servers Menu



RADIUS Authentication Servers

The following figure shows a screen for a RADIUS authentication server.

Figure 123 RADIUS Authentication Servers

☒ **Enable Access to RADIUS Authentication**

☐ Remove Suffix from User ID (e.g. jsmith@nortelnetworks.com)
 Delimiter Value=

RADIUS Users Obtain Default Settings from the Group

Server-Supported Authentication Options

Enabled	Type	Description
☐	CHALLENGE	Challenge/Response Token Cards
☐	RESPONSE	Response Only Token Cards
☐	MS-CHAP	MSCHAP - Microsoft encrypted CHAP. ☒ RFC-2548 (Microsoft Vendor-specific RADIUS Attributes) compliant
☒	CHAP	CHAP - Challenge Handshake Authentication Protocol.
☒	PAP	PAP - Password Authentication Protocol.

RADIUS Servers

Enabled	Server	Host Name or IP Address	Interface	Status	Port	Secret	Confirm Secret
☐	Primary		☒ Private (10.0.16.148) ☐ Public 132.168.2.3	Not Configured	1645		
☐	Alternate 1		☒ Private (10.0.16.148) ☐ Public 132.168.2.3	Not Configured	1645		
☐	Alternate 2		☒ Private (10.0.16.148) ☐ Public 132.168.2.3	Not Configured	1645		

Response Timeout Interval (seconds)

Maximum Transmit Attempts

Diagnostics

[RADIUS Diagnostic Report](#)
 Click here to test for proper configuration of RADIUS authentication parameters.

Enable Access to RADIUS Authentication

Click to enable access to the RADIUS Authentication servers.

Remove Suffix from User ID

Click to remove the user's fully qualified ID suffix from the UID before sending it to the RADIUS server. You do not need the fully qualified User ID if the DNS server has been properly configured on the Switch. A User ID and suffix, where Rcole is the UID and acme.com is the suffix, is Rcole@acme.com

Delimiter Value

Specify the character that separates the suffix from the UID.

RADIUS Users Obtain Default Settings from the Group

Click the drop-down list box to select the default Group from which authorization and operational settings are taken. Any user authorized against a RADIUS server acquires the attributes of this group by default.

If the RADIUS server returns a valid group identifier, the Switch then uses this Group for the user profile. Otherwise, the Switch uses the default Group.

Server Supported Authentication Options

Enabled

Click to Enable server support each authentication type that your RADIUS Server supports and that you expect to use:

- CHALLENGE – Challenge/Response authentication, for example AXENT OmniGuard/Defender
- RESPONSE – Response Only authentication, for example Security Dynamics SecurID.
- MS-CHAP – Microsoft Challenge Handshake Authentication Protocol encrypted authentication
- RFC-2548 Compliance – Check this box to enable the Switch to interoperate with a Microsoft RADIUS Server Version 2.2 or later, or a Version 2.1 with the Microsoft Hotfix applied. Leave this box empty if using a Microsoft RADIUS Server V2.1 (without the Hotfix) or earlier
- CHAP – Challenge Handshake Authentication Protocol authentication

- PAP – Password Authentication Protocol

RADIUS Servers

Enabled

Click to enable the RADIUS servers you want to use for authentication. You can enable up to three servers. The Primary Server receives all RADIUS authentication inquiries unless it is out of service. A RADIUS server that fails to respond five times is temporarily taken off the server list for 30 minutes. After 30 minutes, the server is tried again.

In the event that the Primary Server is unreachable, the Switch queries the first and second alternate RADIUS servers.

Select your RADIUS servers by supplying the Host Name or IP Address, Interface type, Port number, and Password. After configuring the servers, the Switch reports the current server status.

Host Name or IP Address

Enter either the Host Name or IP Address of the servers. For example, Finance.mycompany.com or 145.22.120.111. You can also use simple names (for example, finance) if you have a DNS server configured on your Switch.

Primary

Enter the Primary RADIUS Server host name. This is a required selection if RADIUS is enabled. The Primary server is normally used to process incoming authentication requests.

Alternate 1

Enter the Alternate 1 RADIUS Server host name (this server processes incoming authentication requests if the Primary RADIUS server is unavailable).

Alternate 2

Enter the Alternate 2 RADIUS Server host name (this server processes incoming authentication requests if the Primary RADIUS Server and the Alternate 1 Server are unavailable).

Interface

Specify whether you want the RADIUS server to be accessed via the Switch's private or public interface. The address of the specified interface is used to configure the RADIUS Client address information on the remote RADIUS Server.



Note: Be sure you have enabled RADIUS authentication as an allowed service on the Services→Available screen.

Private

Select Private if the RADIUS server is reached through the private interface. The Switch's management address is used.

Public

Select Public if the RADIUS server is accessed through the Switch's public interface. You must also specify the IP address for the Public interface. The public IP address list is dynamically built from the information on the System→LAN screen. Any change, such as removing an interface card or changing an IP address, is automatically reflected in the drop-down list.

Port

Enter the Server Port Number that you want the RADIUS authentication requests to use. Default is Port 1645.

Secret

All RADIUS Servers share a secret with the Switch. To enhance overall security, this secret should be different for each server. The shared secret encrypts the password between the Switch and the server when the tunnel connection uses PAP or SecurID. It also verifies the authenticity of each accounting request sent by the Switch to the RADIUS server. Furthermore, it verifies the authenticity of each response sent by the RADIUS server to the Switch.

Confirm Secret

Reenter the server's Secret (password) to verify that you typed the password correctly.

Response Timeout Interval

Enter the frequency, in seconds, that you want the Switch to wait before retrying to connect to the RADIUS servers. By default, the Switch tries once every three seconds. The minimum setting is 1.

Maximum Transmit Attempts

Enter the number of times you want the Switch to attempt to connect to the RADIUS servers before failing. By default, the Switch tries three times.

Diagnostics

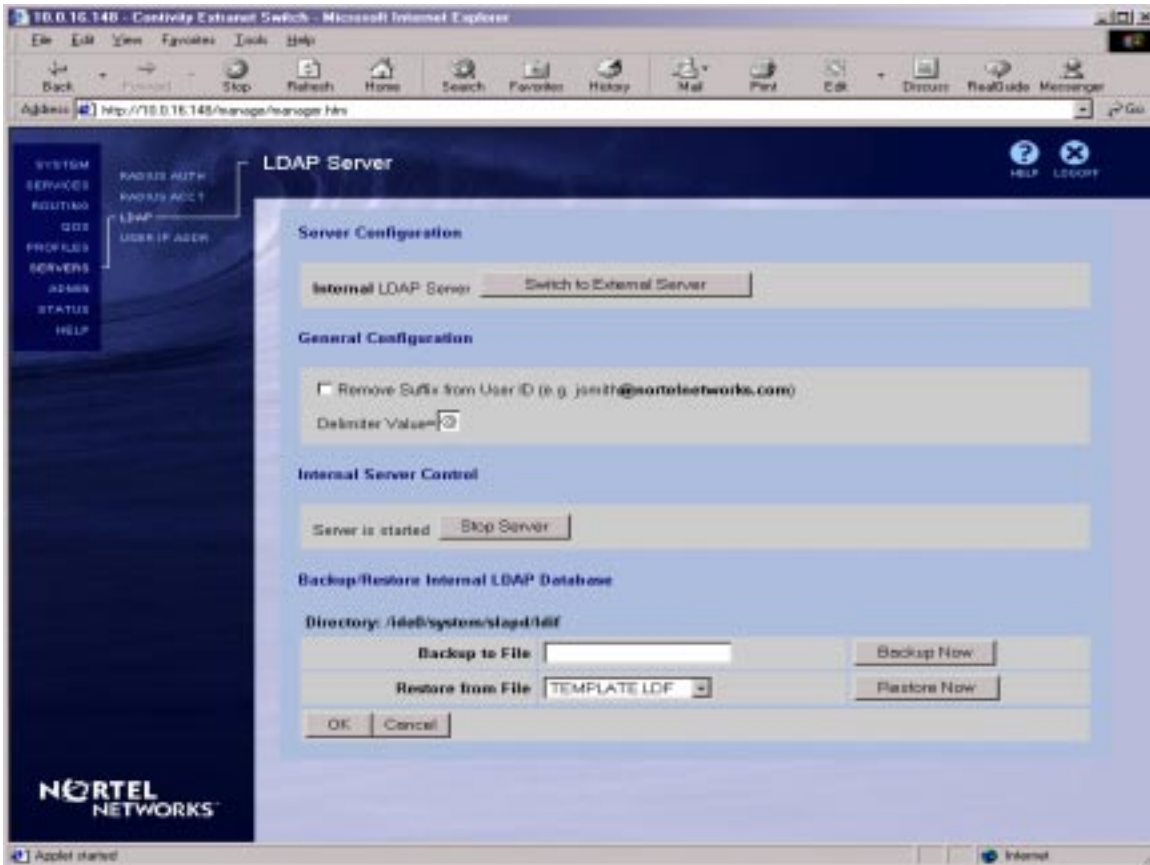
RADIUS Diagnostic Report

Use the RADIUS Diagnostic Report test to check that your RADIUS Authentication configuration is correct. The RADIUS Diagnostic Report compares the settings you have entered on the RADIUS Authentication screen to the corresponding settings that are specified on other Switch configuration screens. The title of each section of the diagnostic report lists the name of the related screen. For example, the IPSec RADIUS Configuration section of the report contains information related to the Services→IPSec screen. Refer to Status→Reports for a more detailed description of the RADIUS Diagnostic Report.

Internal LDAP Server

The Group and User Profiles are stored on the internal server of the Switch.

Figure 124 Internal LDAP Server



Server Configuration

Internal LDAP Server

The Internal LDAP server is internal to the Contivity VPN Switch. If you are using more than one Contivity VPN Switch or if you are using LDAP authentication for other network services, you should consider using an external LDAP server. Refer to External LDAP” for additional information.

Switch to External Server

Click to enable access to the External LDAP server.



Note: The internal server is disabled if you enable an external LDAP servers.

General Configuration

Remove Suffix from User ID

Click to remove the user's fully qualified ID suffix from the UID before sending it to the RADIUS server. A User ID and suffix, where Rcole is the UID and acme.com is the suffix is Rcole@acme.com.

Delimiter Value

Specify the character that separates the suffix from the UID.

Internal Server Control

Click Stop Server or Start Server, as appropriate, when you intend to Back up or Restore a configuration, or after you have completed the restoration of a configuration.



Note: The LDAP server must be stopped before you can perform the Backup and Restore procedures.

Backup/Restore Internal LDAP Database

Directory

Shows the current directory path, which begins at the root disk drive (ide0).

Backup to File

Enter a filename (eight characters maximum) to back up the database, and click Backup Now to start the backup procedure. This procedure backs up changes to the internal LDAP LDIF file only (it writes to the LDAP Interchange Format file). The LDIF file is an intermediate database file that you can use to move data between LDAP servers.

Restore from File

Click the drop-down list box and select a file with which to restore the LDAP database, and click Restore Now.



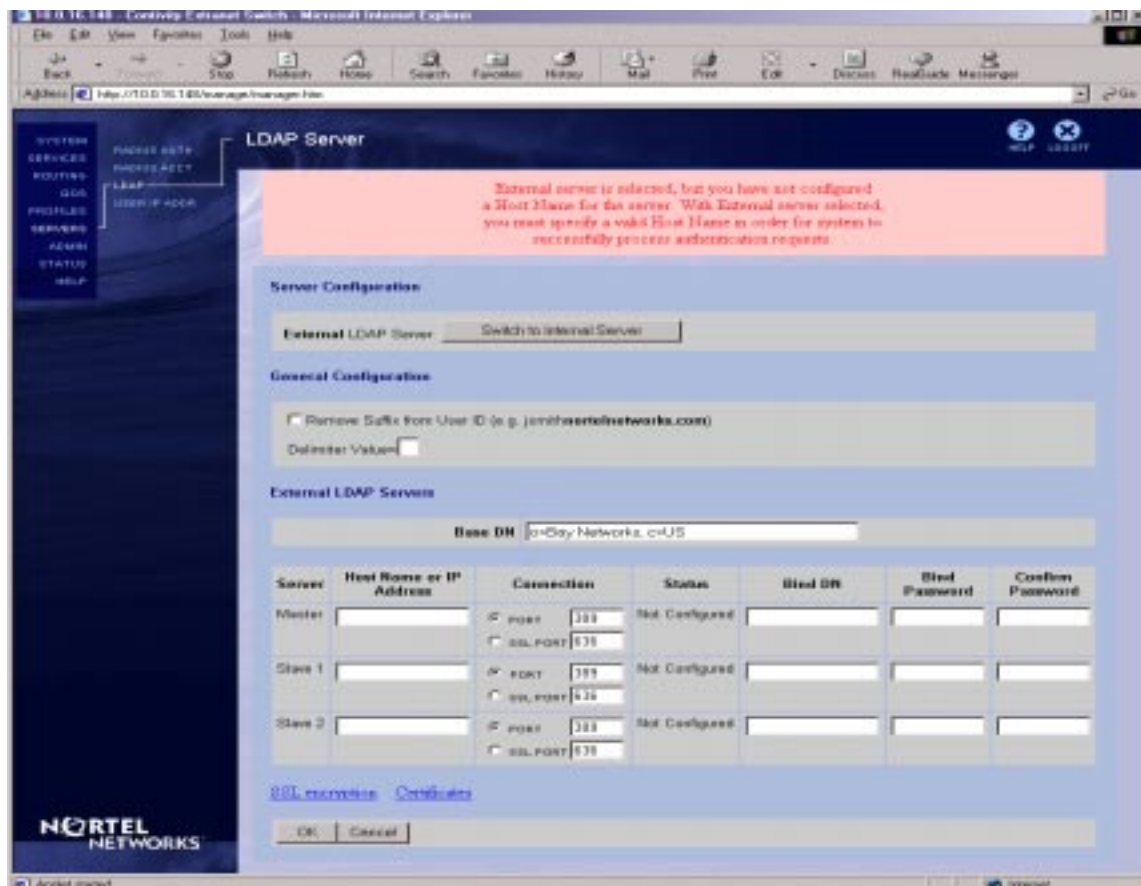
Note: Both the Backup and Restore processes might take extended periods of time, based on the size of the database.

Make sure the LDAP server has been stopped before performing a Backup or Restore procedure. To resume operation of the Switch, you must restart the LDAP server you were running.

External LDAP

The Group and User Profiles are stored on an External LDAP servers.

Figure 125 External LDAP Server



Server Configuration

External LDAP Server

The External LDAP server allows you to configure a Master and two Slave servers. LDAP Slave servers are normally configured to be read-only. In the event that the Master is unavailable, the Switch continues to check against the Slaves for authentication. Configuration writes are not possible while the Master is unavailable.

Switch to Internal Server

Click to enable access to the Internal LDAP server. The external server is disabled if you enable an internal LDAP server.



Note: Status messages appear at the top of the screen to prompt you for a required action, such as entering a valid Host Name.

General Configuration

Remove Suffix from User ID

Click to remove the user's fully qualified ID suffix from the UID before sending it to the RADIUS server. You would not need the fully qualified User ID if the DNS server has been properly configured on the Switch. A User ID and suffix, where Rcole is the UID and acme.com is the suffix, is Rcole@acme.com.

Delimiter Value

Specify the character that separates the suffix from the UID.

External LDAP Servers

Base DN

Enter a Base Distinguished Name (DN) for the servers. A distinguished name is usually in the form of:

`ou=organizational unit, o=organization, c=country`

For example, `ou=Remote Access Users, o=General Motors, c=US`

Server

The remote LDAP servers require the following specifics that are necessary for the Switch to access the appropriate Master and Slave Remote LDAP servers.

Master

The Master LDAP server is the primary server to process queries. Should the Master server become unavailable, the Switch attempts to initiate a connection with the Slave servers. In this case, the Switch tries to reestablish authentication services with the Master LDAP server every 15 minutes, or whenever a request is made to perform a configuration write.



Note: Only the Master LDAP server has read and write access.

Slave 1

The Slave 1 LDAP server responds to queries if the Master LDAP server is unavailable. This server is read-only.

Slave 2

The Slave 2 LDAP server responds to queries if the Master LDAP server and Slave 1 are unavailable. This server is read-only.

Host Name or IP Address

Enter either the host name or IP address for the LDAP servers. These host names can be fully qualified domain names, or simply names if they are in the same domain as the Switch. The entry can alternatively be an IP address.

Connection

Port

Enter the associated Port number that your LDAP server listens to queries on. Port 389 is the default LDAP port number.

SSL Port

Enter the associated Secure Socket Layer (SSL) Port number that your LDAP server listens to queries on. Port 636 is the default SSL LDAP port number.



Note: If you want to use SSL, then you must enable the SSL Port. Additionally, you need to configure the SSL Encryption and Certificates screen options.

Bind DN

The bind distinguished name (DN), which is the LDAP equivalent of a user ID, is required to access the Base DN and its subentries; for example,

cn=Directory Manager

Leave this field blank if your LDAP server allows anonymous access.

The LDAP server must allow read access for the base DN and all its subentries to authenticated connections that are using this bind DN. It must also allow write access for the master server.

Bind Password

Enter a password of up to 32 characters. The password allows the Switch to prove its identity (the bind DN) to the LDAP server.

SSL Encryption

This hyperlink brings you to the LDAP server SSL Encryption screen. This allows you to select the encryption types the Switch uses during negotiation with the external LDAP server. If the external LDAP server does not support one of the selected encryption types, then the connection is not established.

Certificates

This hyperlink brings you to the LDAP server Certificate Configuration screen. This allows you to select the Certificate Authorities (CA) that are trusted to sign the external LDAP server certificates. SSL connections established to an external LDAP server whose certificate is not signed by one of the trusted CAs are dropped.

RADIUS Accounting Configuration

The RADIUS Accounting configuration screen allows you to specify how your Switch saves RADIUS Accounting results. By default, the results are stored locally. You can optionally also save the RADIUS Accounting information to a remote RADIUS Server.

Figure 126 RADIUS Accounting Configuration

RADIUS Accounting

SYSTEM
SERVICES
PROFILES
SERVERS
TUNNELS
ADMIN
STATUS
HELP

RADIUS AUTH
LDAP
RADIUS ACCT
USER IP ADDR

Internal RADIUS Accounting

Enable ☒

Session Update Interval 00:10:00 (hh:mm:ss)

External RADIUS Accounting Server

Interim RADIUS Accounting Record

Enable ☐

Interim Update Interval 00:10:00 (hh:mm:ss)

RADIUS Server

Enable	Host Name or IP Address	Status	Port	Secret	Confirm Secret
☒	10.0.16.247	Error	1646		

OK Cancel Test Server

NORTEL NETWORKS

Internal RADIUS Accounting

Enable

Click to enable or disable Internal RADIUS Accounting. Internal RADIUS Accounting is Enabled by default.

Session Update Interval

Enter an Interval when a snapshot of the current active tunnel sessions is recorded in a journal file. Use the format, hh:mm:ss, for the Interval. The journal file stores the session information until the user logs out of the tunnel session, after which the session stop record is saved on the local disk. In the event of a system crash, upon reinitialization the Switch translates the journal file into a series of stop records on a per session basis. This minimizes accounting data loss. A low interval creates system overhead and requires additional processing.

The default interval is 00:10:00 (10 minutes).

External RADIUS Accounting Server

The Switch can send RADIUS Accounting active session interim start and stop records to an external RADIUS Server. These interim records provide information about the currently active sessions on the Switch. An administrator might use this information to evaluate Switch usage, such as connection start and stop times.

You provide information identifying the external RADIUS server and specify how often the accounting information is sent to the external server.

Interim RADIUS Accounting Record

Enable

Click to enable or disable the Interim RADIUS Accounting Record feature. This selection is Enabled by default.

Interim Update Interval

Enter the Interval at which time interim RADIUS records are sent to the specified external RADIUS Server. Use the format, hh:mm:ss, for the Interval. A frequent interval creates system overhead which requires additional processing. The default interval is 00:10:00 (10 minutes).

RADIUS Server

Enable

Click Enable to specify that the Switch send its accounting records to the external RADIUS Accounting Server.

Host Name or IP Address

Enter the external RADIUS Server's Host Name or IP Address. If you enter a Host Name, use a fully qualified domain name; for example Finance.mycompany.com.

Port

Enter the Server Port number that you want the RADIUS Accounting requests to use. Default is Port 1646.

Secret

Enter the external RADIUS Server's required Secret (password).

Confirm Secret

Reenter the remote server's Secret (password) to verify that you typed the password correctly.

Test Server

Use the Test Server button to verify the connectivity from your Switch to the external RADIUS Server.

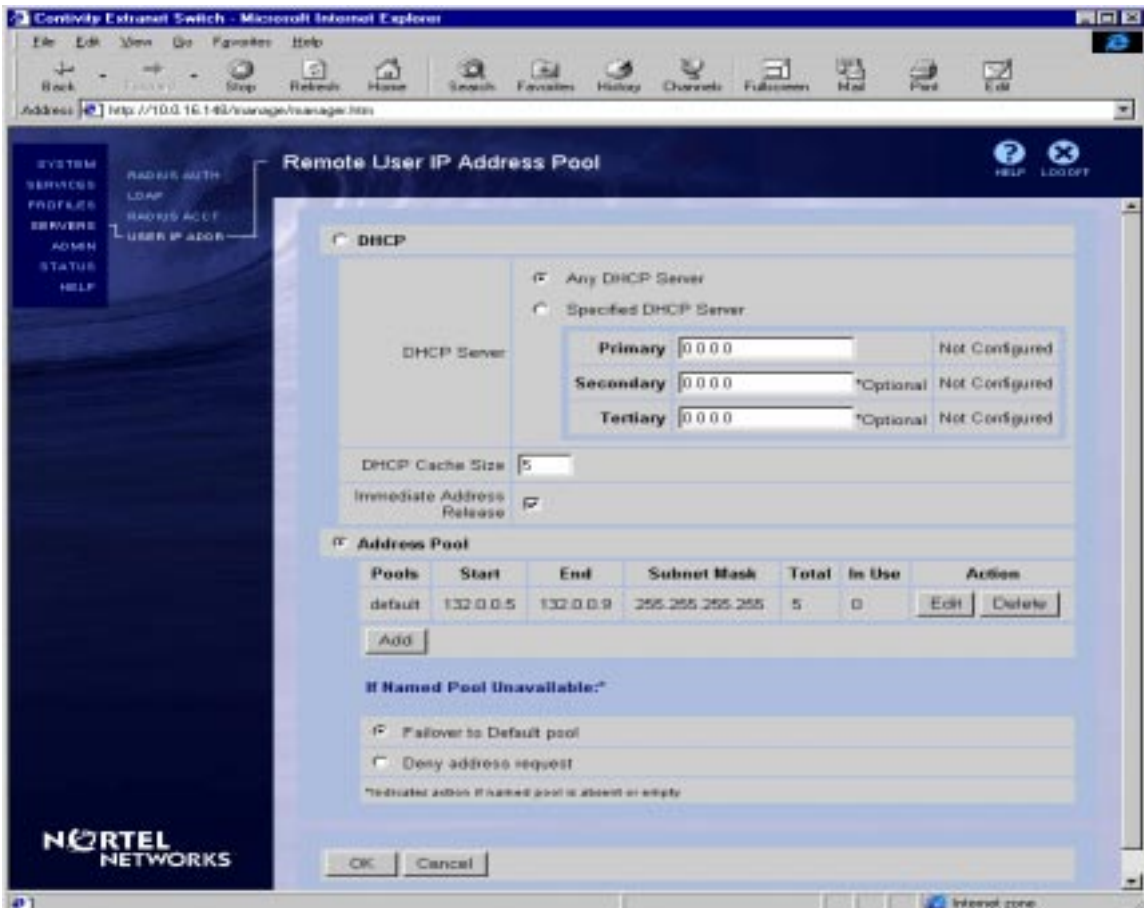
Click to test the connection to the external server. A message at the top of the screen shows the results of the test.

Remote User IP Address Pool

The Remote User IP Address Pool (Servers→User IP Addr) screen allows you to select a method for users to obtain IP addresses for access to the private network. These addresses are serviced by the Switch and are available to remote users accessing the Switch on demand. You can choose to have IP addresses assigned from one of the following:

- External Dynamic Host Configuration Protocol (DHCP) pool
- Internal Address Pool

Figure 127 Remote User IP Address Pool



DHCP

Click to enable an external DHCP server to provide addresses for the address pool. A DHCP server on the private LAN segment dynamically assigns IP addresses on behalf of remote users. You must have an existing DHCP server in your environment to choose this option.

The DHCP server are contacted by a broadcast or unicast (depending on the option selected) DHCP request through the network adapter associated with the Management IP address.

Any DHCP Server

Click to allow any available DHCP server to provide the requested IP addresses. Any DHCP Server is the External DHCP default selection.

Specified DHCP Server

Click to allow IP addresses to be provided from a Specified DHCP Server only. Indicate the IP addresses of the servers that provide DHCP service, including:

- Primary
- Secondary
- Tertiary

A status field provides information on the associated servers. Configuring a Secondary or Tertiary server is optional.

DHCP Cache Size

The Switch obtains a number of IP addresses from DHCP servers. These IP addresses are maintained in a local DHCP cache. The DHCP Cache Size is the number of IP addresses that is held in the Switch's cache. The minimum number of IP addresses held is five, and the maximum is derived from the maximum number of tunnel sessions that the Switch supports.

DHCP Blackout Interval

Enter the amount of time in seconds that a DHCP address is held in a blackout state before it is returned to the DHCP server or the DHCP cache.

Immediate Address Release

When a tunnel session terminates, the Switch can either release the inner IP address back to the DHCP server or retain it for use by a new tunnel session. Click Immediate Addresses Release to have the Switch release the IP addresses back to the DHCP server immediately. If you have a limited number of IP addresses available, then you should enable this option.

IP addresses from disconnected tunnel sessions remain unavailable for the time you specify (300 to 7200 seconds). This delay prohibits immediate reuse by another user that could represent a security risk.

Address Pool

If you want to share all IP addresses among all users, just use Default pools. If you want to assign some addresses to certain users and groups, you can name your ranges and assign that named range to a groups.

Click to use the internal Address Pool, which appears on this screen. These addresses are held by the Switch and are available to clients on demand. Make sure that you populate the local address pool with enough addresses that are not used by other devices on your network. You can create multiple address pools with different ranges of addresses, and you can have multiple address ranges for the same address pool.



Note: If you attempt to delete an address pool that is in use, a message informs you that it is currently being used.

Pools

You can create a default address pool from which users are assigned an IP address dynamically.

Alternatively, you can click Add to name a specific IP address pool. Refer to Remote User IP Address Pool Add” screen for additional information.

Start/End

Shows the first and last IP address for this group of addresses in the local pool.

Subnet Mask

Shows the Subnet Mask for the for the range of pool IP addresses.

Total

Shows the total number of IP addresses in this group of addresses.

In Use

Shows how many of the total number of IP addresses in this pool are currently in use and therefore unavailable.

Action

Click Delete to remove a group of IP addresses.

Click Add to create a new Internal IP address pool.

Address Pool Blackout Interval

Enter the amount of time (0 to 7200 seconds) that an IP address from disconnected tunnel sessions remain unavailable. This delay prohibits immediate reuse by another user that could represent a security risk. Set this number to zero to allow the address to be immediately reissued.

If Named Pool Unavailable

This parameter specifies the action the Switch takes if a user requests an address from a named pool and there are no addresses available.

Failover to Default Pool

Click to have the request for an IP address serviced by the Default IP address pool when there are no IP addresses available in a requested pool.

Deny Address Request

Click to deny an IP address when there are no IP addresses available in a requested pool. In this case, the request is denied and the tunnel is not established.

Remote User IP Address Pool Add

Enter the necessary Starting and Ending IP Addresses on this screen. And then designate the pool as either default, an additional range of addresses to an existing pool, or a newly named pool.

Figure 128 Internal Address Pool Add

The screenshot shows a web browser window titled "Contivity Extranet Switch - Microsoft Internet Explorer". The address bar shows "http://10.0.16.148/manage/manager.htm". The browser's menu bar includes File, Edit, View, Go, Favorites, and Help. The toolbar contains icons for Back, Forward, Stop, Refresh, Home, Search, Favorites, History, Channels, Fullscreen, Mail, and Print. The main content area displays the "Remote User IP Address Pool --> Add" page. On the left is a navigation menu with links: SYSTEM, SERVICES, PROFILES, SERVERS, ADMIN, STATUS, and HELP. A bracket groups "RADIUS AUTH", "LDAP", "RADIUS ACCT", and "USER IP ADDR" under the "SERVERS" category. The "USER IP ADDR" link is highlighted. The main form is titled "Enter Address Pool Information" and contains the following fields and options:

Starting IP Address	
Ending IP Address	
Subnet Mask	*Optional for IPSEC only
Pool	☒ Default
	☐ Existing myTestPool
	☐ New
OK Apply Clear Cancel	

The Nortel Networks logo is visible in the bottom left corner of the page. The browser's status bar at the bottom shows "Internet zone".

Starting/Ending

Enter the first and last IP addresses for this group of addresses in the pool.

Avoid IP Address Pool Conflicts

When supplying an address pool, make sure that none of the pool addresses are the same as those used for the LAN interfaces or the Management interface IP address. Also, the Switch does not check the IP address supplied by a PPTP client to see if it has been assigned to a LAN interface, Management interface, or address pool.

The Use Client-Specified Address option is disabled by default. To avoid potential conflicts, you can verify the current state of the Use Client-Specified Address option from the Profiles→Groups→Edit→Configure PPTP screen.

Subnet Mask (optional)

This field is applicable to IPSec users only. Enter the Subnet Mask for the pool of IP addresses that you are configuring. You can later edit the Subnet Mask as necessary.

Pool

You can designate the Pool as Default, Existing, or New.

Default

Click to designate this pool as the Switch's Default IP address pool.

Existing

Click to change the subnet mask or name of an existing pool. If you want to edit the IP addresses of an existing pool, you must either delete the pool (if not in use) or click Add and then associate this new pool with an existing pool.

New

Click to create a new IP address pool and then name the pool.

Action

Click OK to save the entries for the IP address pool and return to the Remote User IP Address Pool screen.

Click Apply to save the entries for the IP address pool and remain at the current screen.

Click Clear to clear the entries on the screen.

Click Cancel to return to the Remote User IP Address Pool screen. Any unsaved entries are lost.

Server Farm

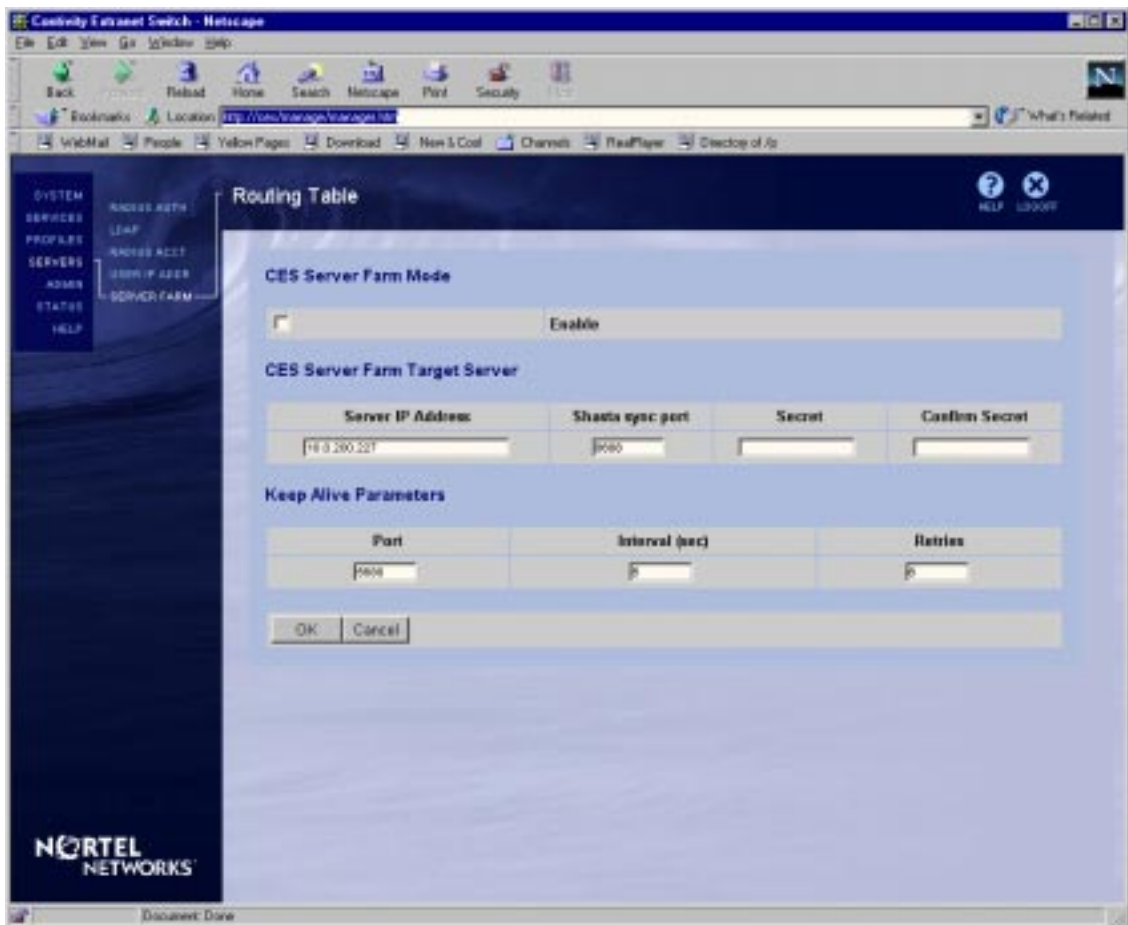
The Server→Server Farm screen allows you to enable and configure parameters for Server Farm functionality. Server Farm functionality is available when the CES is used with a Shasta 5000 Broadband Services Node (BSN).

The Shasta 5000 gives service providers the ability to offer a network-based VPN solution that integrates multiple fixed sites, xDSL connected telecommuters, and dial-in telecommuters via L2TP connected modem pools.

The CES offers Virtual Private Dial Networking (VPDN) capability for enterprises to integrate mobile telecommuters via IPSEC, L2TP, PPTP, or L2F tunnels.

The Shasta 5000 BSN integrated with the Contivity VPDN provides a complete VPN solution for network-based managed VPN services.

Figure 129 Shasta Server Farm



CES Server Farm Mode

Enable

Click the Enable check box to enable Server Farm functionality.



Note: When CES Server Farm Mode is enabled, any dynamic and static routing information previously set is suspended. All traffic is default routed to the Shasta device only.

CES Server Farm Target Server

Server IP Address

Enter the IP Address of the Shasta Server.

Shasta Sync Port

Enter the port number of the Shasta Server.

Secret

Enter the password.

Confirm Secret

Enter the password in this field to confirm it.

Keep Alive Parameters

A Keep Alive mechanism is used between the CES and the Shasta server to detect the failure either one. It is initiated by the CES when you enable Server Farm functionality.

Port

Enter the port number of the Shasta Server.

Interval (sec)

Specify the time interval, in seconds, between keep alive transmissions.

Retries

Specify the number of retry attempts.

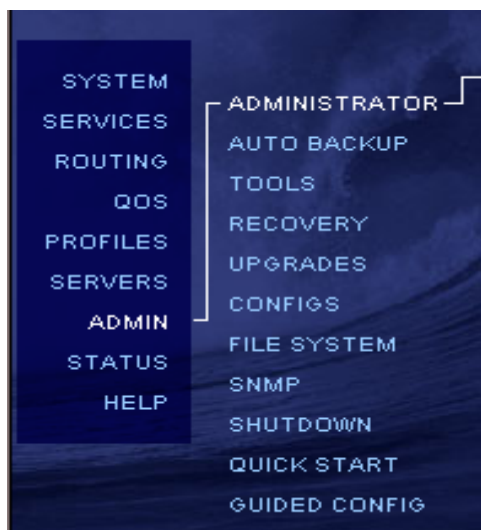
The CES retries 3 times by default. If the CES does not receive acknowledgement within this number of tries, it tears down the tunnel. Note that this tunnel connection is cleared in the Shasta 5000 only when the CES comes back with a new tunnel "start" with this IP address, or when the CES is reset.

Chapter 7

Administration

This section describes Administration tasks that are central to operating the switch. These tasks provide details on scheduling backups, upgrading the software image, saving configuration files, performing file maintenance, creating recovery diskettes, and shutting down the system.

Figure 130 Administration Menu



Also, links allow you to access either the Quick Start Configuration or the Guided Configuration.

Administrator Settings

The Administrator Settings screen allows you to change the Primary Administrator User ID (UID) and Password. It also controls the Administrator Idle Timeout Setting for all administrators, the default language, and serial port settings.

There can be only one Primary Administrator. The Primary Administrator User ID and Password combination provides the person with this information access to all screens and control settings. The Primary Administrator User ID and Password are also used to access the serial port and the recovery disk.



Note: The Primary Administrator UID and Password are only saved during a system shutdown. Therefore, when you set these parameters you must implement an Admin→Shutdown to save the new settings. Doing a Reset (using the Reset Button on the back of the Switch) does not store the parameters.

Figure 131 Administrator Settings

10.0.16.148 - Contivity Extranet Switch - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss RealGuide Messenger

Address <http://10.0.16.148/manage/manager.htm> Go

SYSTEM
SERVICES
ROUTING
QOS
PROFILES
SERVERS
ADMIN
STATUS
HELP

ADMINISTRATOR
AUTO BACKUP
TOOLS
RECOVERY
UPGRADES
CONFIGS
FILE SYSTEM
SNMP
SHUTDOWN
QUICK START
GUIDED CONFIG

Administrator

Primary Administrator

User ID

Password

Confirm Password

Note: Changes to the Administrator User ID and Password take effect only after a proper shutdown.

Settings

Idle Timeout (hh:mm:ss)

Default Language

OK Cancel

NORTEL NETWORKS

Done Internet

Primary Administrator

User ID

Enter an appropriate User ID for the Primary Administrator. The person using this UID has permission to modify and view all control settings in the Switch, including the serial port and the recovery disk.

Password

Enter an appropriate Password for the Primary Administrator.



Caution: Do not lose or forget this Password. Losing or forgetting your Password requires you to return the Switch to Nortel Networks for reconfiguration to default settings. All settings and backups are lost. There is no way to access the system without the Primary Administrator Password.

Settings

Idle Timeout

The Idle Timeout setting is used to force an automatic logout when an administrator session is not in use. This setting controls the timeout for all administrators.

If no interaction with the Switch takes place for the specified time, this option allows you to configure a timeout period after which a dialog box appears asking for the ID and Password. This feature helps prevent someone from accessing and modifying the Switch from an administrator's Web console that has been left unattended.

The default Idle Timeout is 00:15:00 (15 minutes); the range is 00:15:00 to 23:59:59.



Note: If the Idle Time-out on the switch logs off the Client, and the Client has Client Failover configured on the Services→IPSec screen, that client then fails over to the defined failover server, rather than being disconnected as desired.



Note: An option has been added to the Contivity VPN Client to disable keep alives between the switch and the client. This option enables you to disable keep alives when tunneling over an ISDN link, since the link is not always active. If an Idle Time-out has been set on the switch, and keep alives have been disabled on the client, the client might not receive notice that the connection has been closed (due to the Idle Time-out), when the physical ISDN connection is not active.

Default Language

Select the language that you want to use for your Switch's GUI. The Switch supports English and Japanese.

Using Japanese

To display the Japanese screens properly, your Web browser must support Kanji characters. Refer to your browser's documentation for additional details.

The following browsers have been tested and found to provide this support.

- Netscape Navigator, Version 4.0 or later
- Japanese version of Microsoft Internet Explorer, Version 4.0 or later

When you select Japanese, your Switch's GUI is converted from English to Japanese Kanji characters. However, the following types of information are *not* translated into Japanese:

- Text that is entered by a user
- Information from one of the Switch's databases
- Online Help



Note: After you change your Switch's language selection, click on your browser's Refresh button (Internet Explorer) or Reload button (Netscape) to update the browser's screen to the new language.

You may notice that some screens appear in English even though you have selected Japanese. These screens were added after the last Kanji translation was done and will always appear in English.

Install Keys

Use the Admin→Install Keys menu item to install a licensing key that enables optional software functionality.

Key Installation

Feature

The Feature column lists optional features that are currently available.

Key/Status

Enter the key that you obtained from your Nortel Network's sales representative in this text box and click OK. The key must be entered exactly as it is given.

When a valid key is installed the label "Key Installed" appears in this column.

Delete

Click Delete to remove the key. A confirmation page appears. Click Yes to confirm key removal.

Automatic Backup

The Automatic Backup screen allows you to configure regular intervals when your system files are saved to designated host backup file servers. You can designate up to three backup file servers.

You should configure Automatic Backups immediately so that you do not lose system or configuration information in case of problems. You configure the Automatic Backup servers from the Admin→Automatic Backup screen.

The Switch does not begin a backup for at least 5 minutes after rebooting. This time period is to allow all resources to start operating. This delay occurs even if you go into the Admin→Auto Backup screen and request that a backup be started immediately; it is delayed until after the 5-minute period.

Figure 132 Automatic Backup

Enabled	Host	Path	Status	Specific time	Interval (hours)	User ID	Password	Confirm Password
☐				11:48:39	5			
☐				11:48:39	5			
☐				11:48:39	5			

Backup enabled servers: none

OK Cancel



Note: After entering the Automatic Backup File Servers information, click on the screen and press the keys Alt and Print Scrn (Screen) to save the screen image to a buffer. Next, paste the image into a file (for example, into Microsoft Word) and keep it as a record of the backup file servers that you are using.

Restoring Configurations

If you want to save a certain configuration for a later date, you must realize that there are two components that define a given configuration: the configuration file and the LDAP database.

Saving a configuration from the Admin→Configs screen Save Current Configurations option saves only the operational parameters in the configuration file, such as interface IP addresses and subnet masks, backup host IP addresses, and DNS names.

To completely save the Contivity VPN Switch configuration on the internal LAN server, you must also save the LDAP database, which contains the group and user profiles, filters, backup file names, and more. Go to the Servers→LDAP screen and click Stop Server. Next, enter a file name in the Backup/Restore LDAP Database field. Note that you should conform to the eight-dot-three MS-DOS® naming convention and append the file name with .ldf; for example, LDAPOne.ldf.

Automatic Backup File Servers

Enabled

Click to Enable the associated Host Backup File Server.

Host

Enter the Backup File Server Host name or IP address.

Path

Enter the Backup File Server Path, for example:

Building3/Switch_backups

Specific Time

Select this option to execute the backup at a specific time. Enter the time at which you want the backup to occur.

Interval

Select this option to execute the backup at certain intervals of time. Specify in hours the time period after which the system automatically backs up changed files to the backup file server. The minimum interval is 1 hour, and the maximum is 8064 (336 days); the default is 5 hours.

User ID

Enter the User ID that is required for FTP login to the backup file server.

Password

Enter the Password that is required for FTP login to the backup file server.

Confirm Password

Reenter the Password that is required for FTP login to the backup file server.

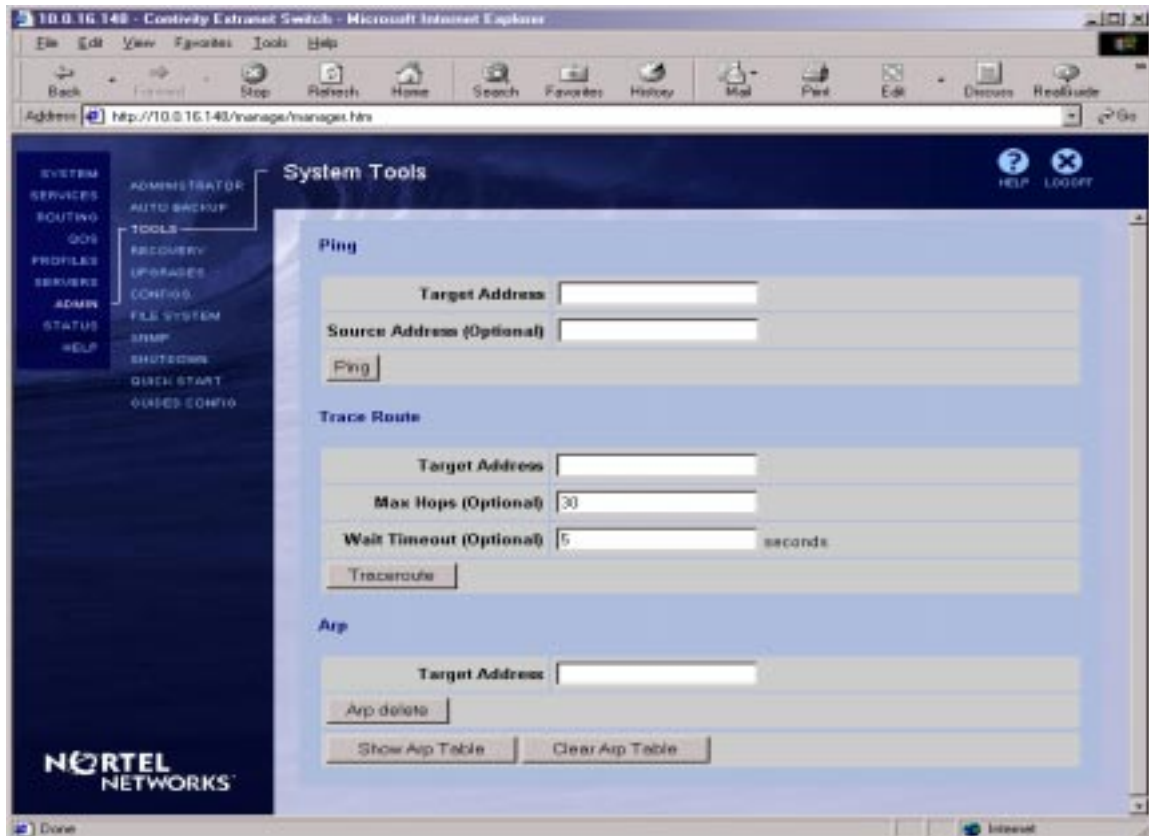
Backup

Click to execute a backup to each enabled server now. This action also synchronizes the hard disk drives when there is more than one in a device. Otherwise, the hard disks synchronize automatically every 60 minutes.

Tools

The Tools screen provides utilities for checking connectivity.

Figure 133 Admin→Tools



Ping

The ping command generates an ICMP echo-request message, which is sent by any host to test node reachability across a network. The ICMP echo-reply message indicates that the node can be successfully reached.

Target Address

Enter the IP address that you want to ping.

Source Address (Optional)

You can optionally enter the address that you are pinging from.

Ping

Click the Ping button to execute the ping.

Traceroute

The traceroute command is a tool used for measuring a network round-trip delay. Messages are sent per hop and the wait occurs between each message. It takes the maximum hops (30) x the wait timeout (5) x 3 seconds for the traceroute to time out if the address is unreachable.

Target Address

Enter the IP address whose route you want to trace.

Max Hops (Optional)

You can optionally enter a maximum number of hops to which to limit the traceroute.

Wait Timeout (Optional)

Enter an optional Wait Timeout value in this field to limit timeouts.

Traceroute

Click the Traceroute button to execute the traceroute.

Arp

The Address Resolution Protocol (ARP) dynamically discovers the low level physical network hardware address that corresponds to the high level IP address for a host. ARP is limited to physical network systems that support broadcast packets that can be heard by all hosts on the network.

Target Address

IP address of system for which you want to delete ARP table entries.

Arp delete

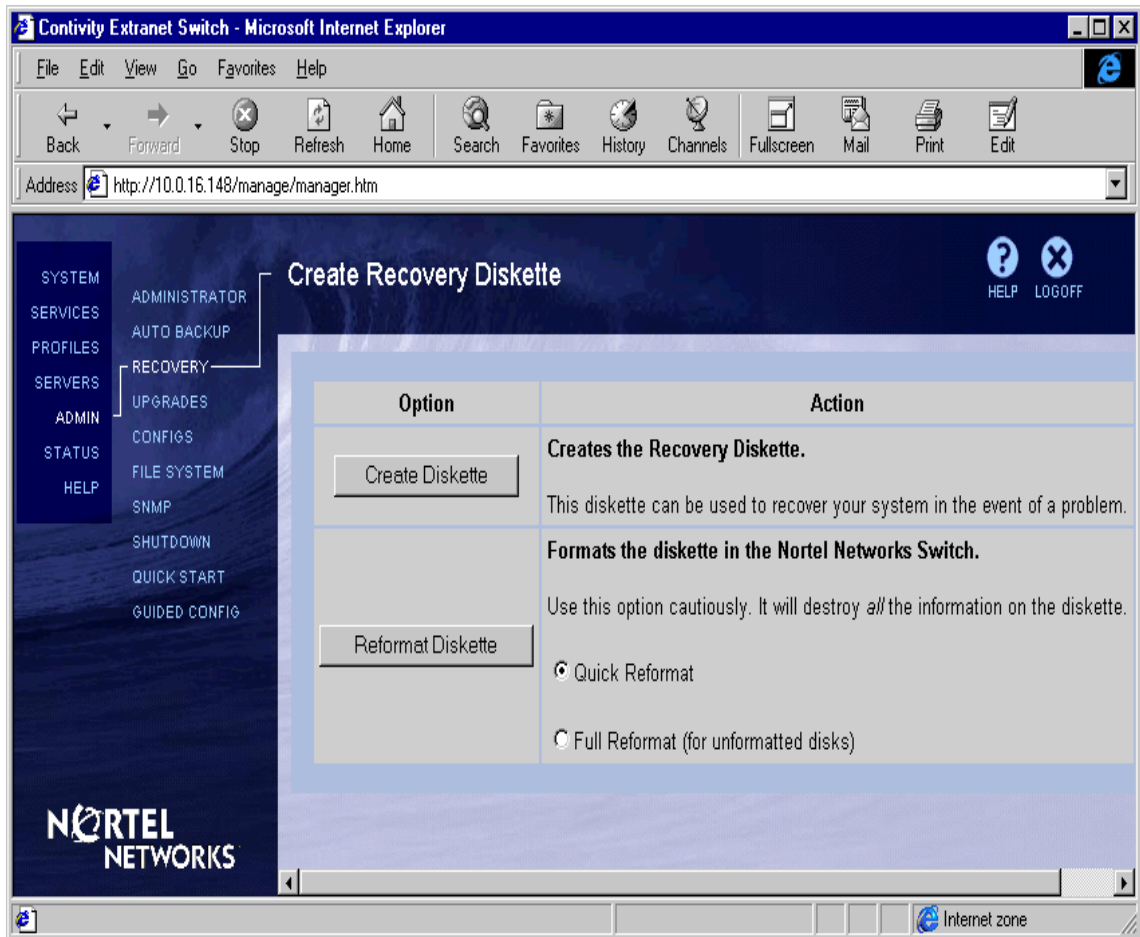
Clicking on this button deletes the specified entry from the ARP table.

Clear Arp Table

Clicking on this button clears all of the existing ARP table entries.

Recovery

The Recovery screen allows you to create a recovery diskette that can enable you to restore the software image and file system to the hard drive of the Switch in the unlikely event there is a hard disk crash. The Recovery diskette is included with your Switch. You can also use this screen to create additional copies of the Recovery diskette, as well as to reformat a diskette.

Figure 134 Create Recovery Diskette Display

Creating Recovery Diskette

Create Diskette

Creates the Recovery Diskette that is used to restore the file system on the Switch's hard drive in the unlikely event of a hard disk problem. This process creates a boot sector on the diskette, and copies the system software files that are necessary to boot the Switch using the diskette.

When the Recovery Diskette creation is complete (approximately 2 minutes), a message appears at the top of the screen indicating success or failure. In case of a failure, follow the instructions in the user messages provided by the Switch.

Reformat Diskette

Formats the diskette in the Switch. Use this option cautiously; it erases all of the information on the diskette.

The options follow:

- Quick Reformat (default for previously formatted diskettes) - Rewrites header files and existing data.
- Full Reformat (for unformatted diskettes) - Creates the data sectors that comprises the storage space.

The system prompts you to verify that you intend to reformat the diskette.

Using the Recovery Diskette

Remove the Switch's front cover (refer to your switch's *Getting Started Guide* for instructions). Insert the recovery diskette into the drive and press the Reset button on the back of the Switch. This supplies the Switch with a minimal configuration utility that allows you to view the Switch from a Web browser.

At your Web browser, enter the Management IP address of your Switch. The Recovery Diskette screen appears, which allows you to:

- Restore the factory default configuration or the backup configuration.
- Reformat the Switch's hard disk.
- Apply a new software version to the Switch.
- Perform file maintenance.
- View the Event log.

Figure 135 Recovery Diskette

Option	Action															
Restore	Restore Factory Configuration ☐ Restore original factory settings: This option resets the Switch's configuration file to the original values it had when shipped from the factory. The system software and internal LDAP database entries will not be altered. Important: If you choose this option, the Switch will need to be reconfigured as if it were new. Restore Backups Restore a backup image from one of the selected servers. When restoring backup files, all configuration files, internal LDAP databases, and system software will be restored from the selected backup directory. This option should only be used to restore (or install) a complete system image to the Switch, and should not be used as a method of upgrading the Switch. Note: To upgrade the Contivity Extranet Switch, use the Admin->Upgrades feature of the management interface. <table border="1"> <thead> <tr> <th>Host</th> <th>Path</th> <th>User ID</th> <th>Password</th> <th>Confirm Password</th> </tr> </thead> <tbody> <tr> <td>☐ 10.9.0.10</td> <td>backup/sn44</td> <td>Administrator</td> <td>*****</td> <td>*****</td> </tr> <tr> <td>☐</td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Host	Path	User ID	Password	Confirm Password	☐ 10.9.0.10	backup/sn44	Administrator	*****	*****	☐				
Host	Path	User ID	Password	Confirm Password												
☐ 10.9.0.10	backup/sn44	Administrator	*****	*****												
☐																
Reformat hard disk	Formats the hard disk in the Switch. Use this option cautiously. It will destroy all the information on the Switch's hard disk. Reformat															
Apply new version	Changes the version of software executing on the Switch. Use this option to change to other software versions which exist on the Switch's hard disk. To retrieve new versions, use the Admin->Upgrades feature of the management interface. When applying a new software version, the current version will be preserved under a unique name. Select the desired software version: (No version selected) ▾															
Perform file maintenance	Presents a listing of directories and files on the Switch. Files															
View event log	The Event log allows you to see system Events that have occurred on the Switch. This log should be used to resolve problems that occur when trying to use the various options of the Recovery diskette. View															
Restart system	To restart the system, remove the diskette and press the Reset button on the back of the Switch. Refresh															

Restore

Restore to Device

Select the hard disk drive to which you want to restore the system files; either ide0 (drive 0) or ide1 (drive 1).

Restore Factory Configuration

Click Restore Factory Configuration, then click Restore to return the Switch to its original factory default configuration. This erases data contained in flash memory and also in the configuration file.



Caution: Selecting this option requires you to rebuild your entire Switch configuration again from scratch.

An online message specifies the result of the Factory Configuration reset action.

Restore Backups

Click to restore the Switch's previously backed-up configuration. If you previously chose to automatically backup (refer to Automatic Backup") the file systems, then the Backup Server Host (or IP address) and Path Name, User ID, and Password appear in the table.

Click the radio button of the preferred backup server. The backed-up file system, including software image and configuration files from the latest backup copy residing on the designated server, is restored onto the hard drive of your Switch.

You can use the same backup server for multiple Switches. Each Switch creates a unique directory based on its serial number. The following example shows the Host, Path, and Serial Number (where the serial number [SN] is five digits):

```
C:/software/backup/v101/SN01001
```

Refer to the example in "Backup Servers" for additional details on the directory, host, path, and serial number string.

Backup Server and Serial Number

The Serial Number is used to differentiate backup configurations from multiple Switches that are saved on the same backup server. The Serial Number uniquely identifies each Switch's backup data.

A blank row in the server backup field always appears to allow you to manually enter a backup server in case you did not configure automatic backup server locations.

Alternatively, a new factory default software image and file system can be restored to the Switch's hard disk. Specify the name or address and path of the network file server onto which the software from the Nortel Networks CD has been installed.



Note: This restores the disk to an operable but “clean” condition (configuration values are at factory defaults).

To view your Switch's Serial Number when the Switch is operational, click Status→System from the Navigational Menu. The Serial Number is also listed on the bar code label on the back of the Switch.

Reformat Hard Disk

Click to Reformat your Switch's Hard Disk. Following are instances when you might need to Reformat the Hard Disk:

- If you have problems restoring your configuration that are not caused by the network or the file/backup server from which the file restoration is being retrieved
- If you want to reconfigure the Switch from scratch
- If you install a new disk



Caution: Selecting this option completely wipes out anything that previously resided on the hard disk.

An online message indicates whether the Reformatting of the Hard Disk was successful.

Apply New Version

Click the drop-down list box to view the available software image and file systems that are currently stored on the hard disk. Select the image version that you want to activate.

This selection is applicable if you have more than one version of software available on the Switch.

Perform File Maintenance

Click Files to bring up the File Maintenance screen, which allows you to view the entire hard disk file system.

View Event Log

Click View to display the Event Log beneath the Recovery Diskette screen. This is especially useful if a Restore operation fails.

Set Boot Disk

Click the drop-down list box to select the hard disk drive from which you want to boot the Switch; either ide0 (drive 0) or ide1 (drive 1). Then click Set.

Synchronize Disks

Click Synchronize to immediately synchronize the primary and secondary disks. Thereafter, the disks automatically synchronize every hour.

Upgrade System Boot Software

Click the drop-down list box to select a drive onto which you want to update the system boot software. Click Upgrade to rewrite the boot software onto the hard disk. You would do this if the system boot sector were to become corrupted.

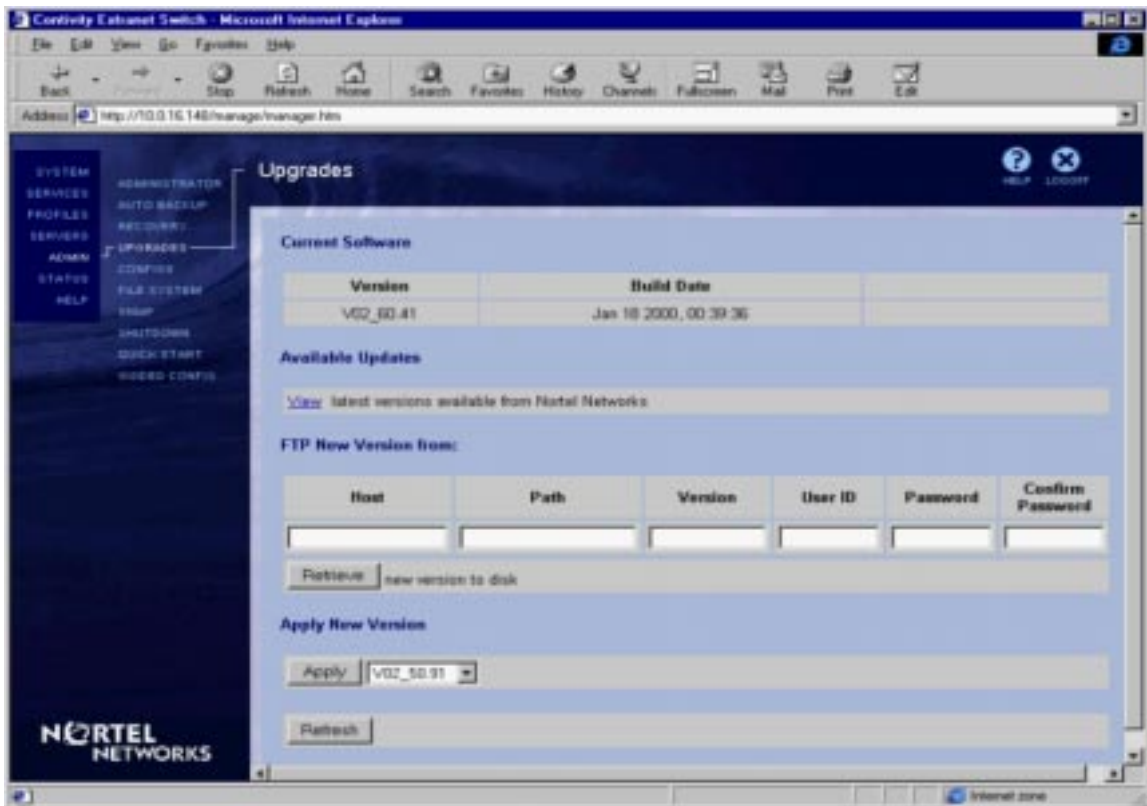
Restart System

Remove the diskette and press the Reset button on the back of the Switch. Then reposition your Web browser to the Management IP address, and choose Reload or Refresh from your browser menu to access the management page of the software running on the hard disk.

Upgrades

The Upgrades screen allows you to download the latest Nortel Networks software for the switch via File Transfer Protocol (FTP). In addition to retrieving software you can select which version of software to run.

Figure 136 Upgrades



Current Software

Version

The current Version of software running on the Switch.

Build Date

The Build Date of the current Version of software running on the Switch.

Available Updates

View

Click to go to the Nortel Networks Web site to determine which software versions are available.

FTP New Version From

If necessary, enter a Host server and its required access information to allow you to retrieve the latest software images for your Switch.

Host

If necessary, enter the name or IP address of the Host remote server that contains the Switch software version to be retrieved.

Path

If necessary, enter the path to the directories and files where the Switch software image is stored.

Version

Enter the software image file Version that you want to download to your Switch. Typically, you would enter the latest software Version. However, if you had a problem with a current version and you wanted to revert to an older version, you could do so here.

To determine the latest version of software, check the Version number in the title of the software release notes. Or, you can click View to visit the Nortel Networks Web site to find the latest software version. Contact Nortel Customer Support for additional information.



Note: To operate with the latest version of software, you must first download it, and then select Apply New Version (see below).

User ID

If necessary, enter an appropriate User ID for the FTP server.

Password

If necessary, enter the FTP server Password.

Confirm Password

If you entered an FTP server password, reenter the password to verify it.

Retrieve

Click Retrieve to download the software image file for the Switch. The download takes several minutes, and upon completion, the Upgrades screen reappears with a success or failure message.

Apply New Version

Version to Apply

Click the drop-down list box to view the software versions that are available on your system. Select the version that you want to run on the system.

Apply

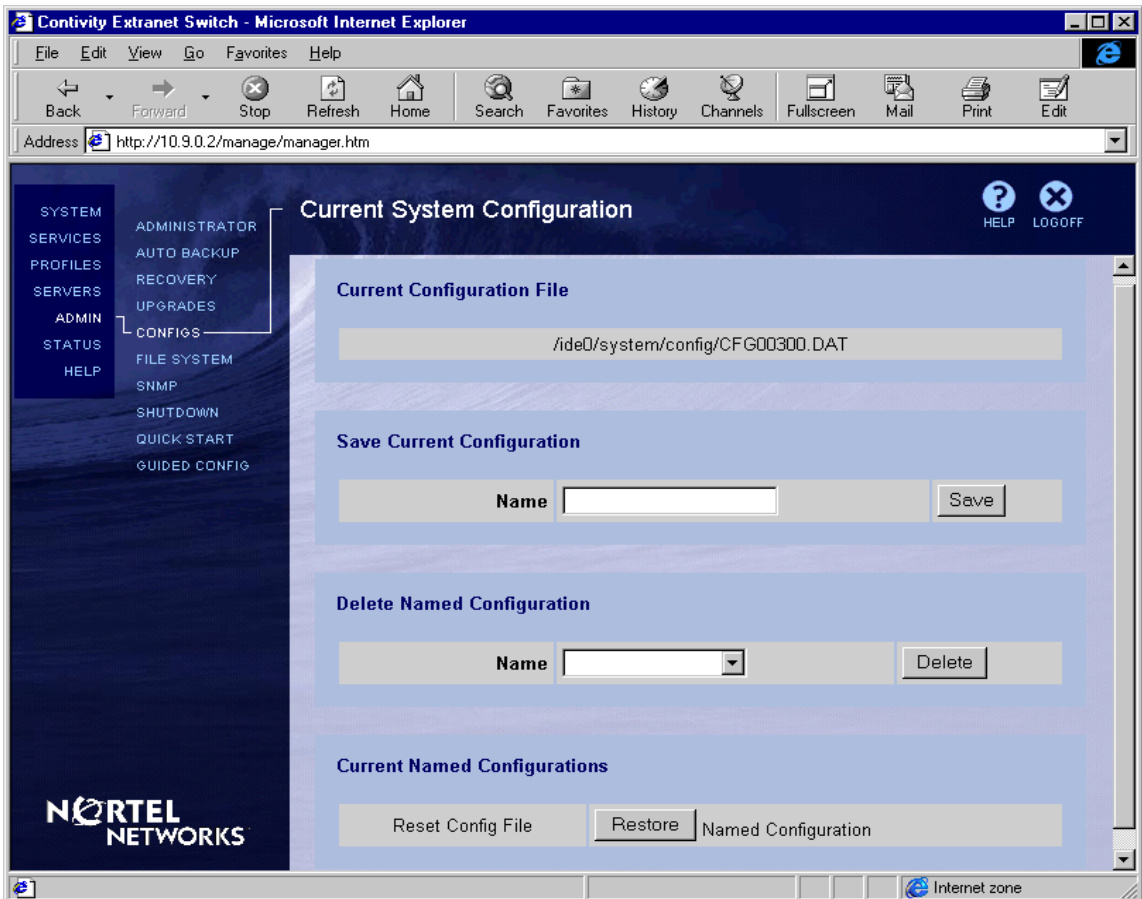
After you select the new version, click Apply. This restarts the system with the version that you now want to run on the Switch.



Note: After you apply the upgrade, you should purge your browser's cache. This clears old references to screens that might have changed between versions.

Current System Configuration

The Admin→Config screen allows you to Name and save the Current System Configuration. Additionally, you can select one of the previously named configurations and restore it to be the Current Configuration.

Figure 137 Current System Configuration

Save Current Configuration

Name

Enter a date as the Name for the Current software Configuration; for example, April 15, 1999.

Save

Click to Save the Current software Configuration name.

Delete Named Configuration

Click the drop-down list box to display the name of the Configuration that you want to delete.

Current Named Configurations

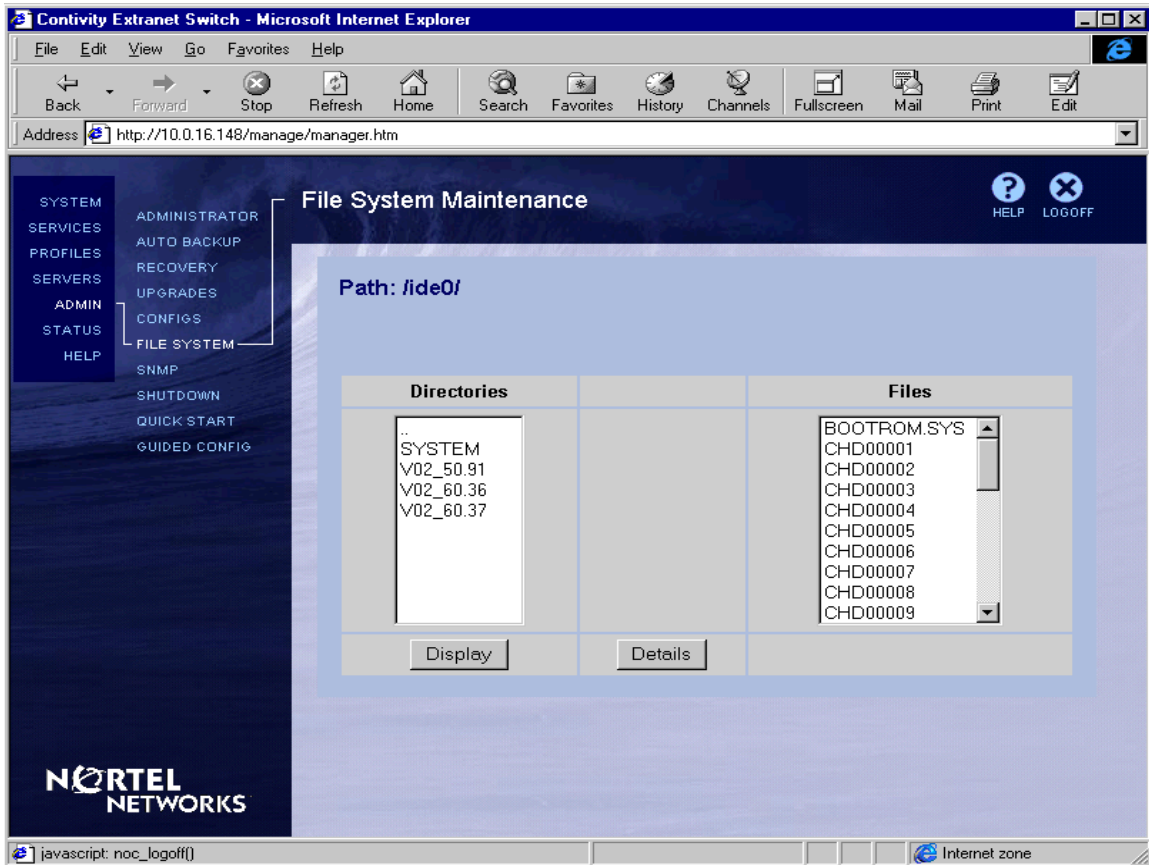
Restore

Click the Restore button to go the System Shutdown screen. From there, click the drop-down list box Under Boot Configuration to select a configuration to be restored as the Current Configuration after a reboot.

File System Maintenance

The File System Maintenance screen allows you to navigate through the Switch file system. The top level lists the devices (drives), and beneath a given drive are the directories. This provides flexibility in viewing details of a file or directory, and it allows you to delete unnecessary files. For example, if you had problems performing an FTP transfer with a specific file, you could view the file details to learn its file size and when it was last modified for troubleshooting purposes. Additionally, you can toggle between hard drives when a backup drive is available.

Figure 138 File System Maintenance



Devices

This field applies to the 4000 series Switches, which have two hard disk drives. This field appears only when you are at the top level of the file structure; when the hard drives and floppy drive appear in the column. To get to this level, select the two periods (..), then click Display.

Action

Click to Enable or Disable the associated hard disk drive, either ide0 (drive 0) or ide1 (drive 1). Clicking either of these buttons turns the drive online or offline. When the Switch boots it makes sure the primary disk is not corrupt; if it is corrupt, then the Switch boots from the secondary disk.

If you receive error messages about the secondary drive, disable it so that the synchronization does not even try to read or write to the drive.

Click Enable to activate the listed drive (for example, ide1 – drive 1).

Click Format to reformat the listed drive (for example, ide1 – drive 1). Use this action with discretion, as you would completely wipe out data existing on this drive.

Display

Click on the Directory that you want to view. Next, click Display to change the path to the selected directory.

Details

Click to display the associated Directory or File information. Clicking Details also invokes the Delete option. The Delete option allows you to delete a single file or the contents of an entire directory. Refer to “File System Maintenance Details” for additional information.

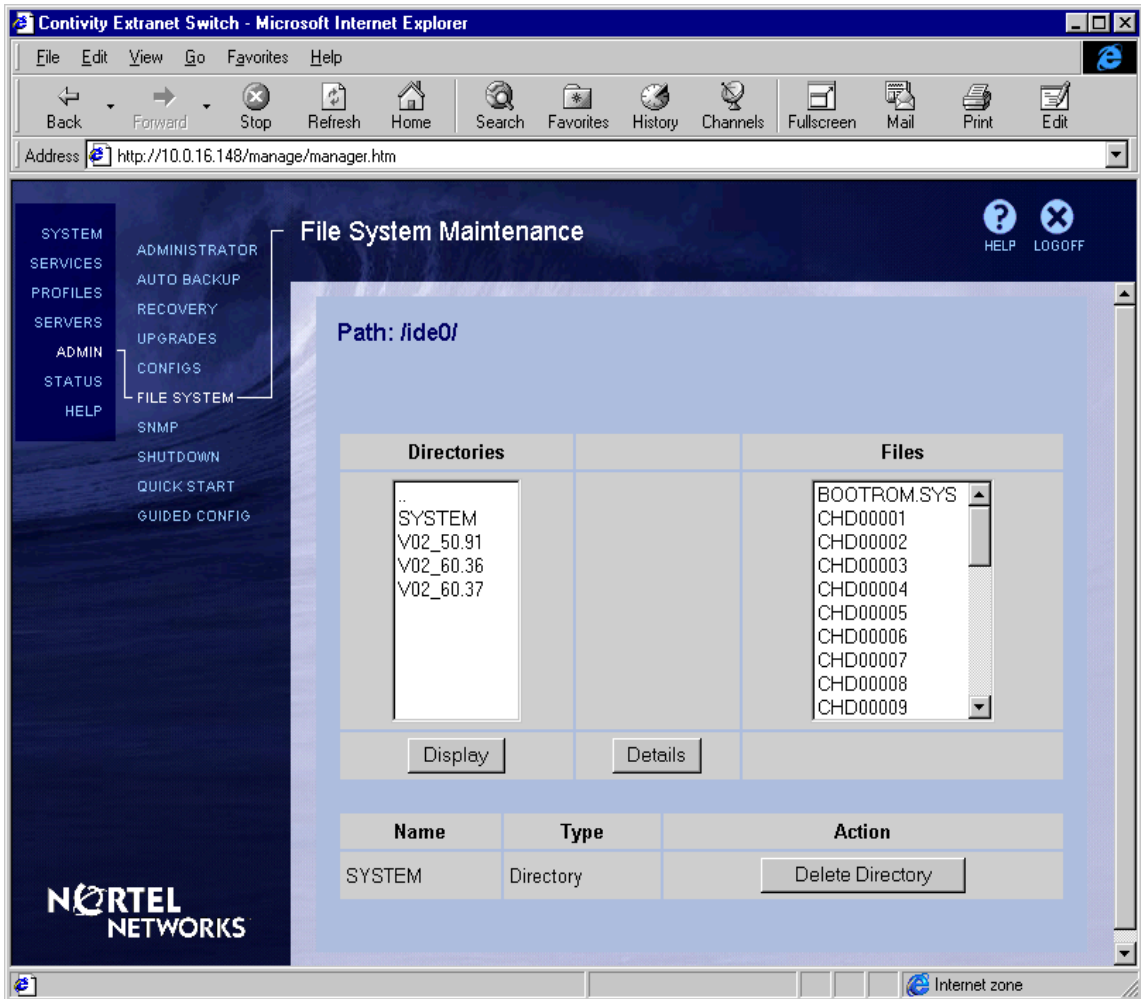
Prepare

Click to Prepare the selected hard disk drive for removal. This clears the system cache of the selected drive's contents. Not preparing the hard disk drive for removal presents the risk that there could be file corruption upon reinsertion of the drive. Additionally, this prevents any possibility of inaccurately accessing data from the drive that was previously in use.

File System Maintenance Details

This screen provides the details associated with a selected directory or file.

Figure 139 File System Maintenance Details



Name

The name of the selected File; for example, bdy_boot.htm.

Type

Shows whether the selected details are from a file or a directory.

Size

The file size, in bytes.

Date

The Date the file was created (mm/dd/yyyy).

Time

The Time the file was created (hh/mm/ss).

Action

Delete Directory/Delete

Click to Delete the contents of a Directory or an associated file. If you choose to Delete a Directory, all of the files in the directory are deleted. Only users with Administrator Rights to Manage the Switch can delete files or directories.

The system prompts you to verify that you intend to delete the contents of a Directory (and Directory Name), or selected file.

SNMP

The SNMP screen allows you to generate SNMP Version 1 Traps, based on MIB II. Use this screen to do the following:

- Designate the remote SNMP management stations that are authorized to send SNMP Gets to the Switch.
- Designate the trap hosts to which the traps can be sent.
- Configure the traps.

The SNMP counters measure packet attributes that are based on the outer IP header. In the tunneled environment there is also an inner IP header, but this IP header does not contribute to the SNMP MIB counters. For example, the outer packet header might be a good packet header and be counted, but the inner packet header might be corrupted and would not contribute to the drop counter.



Note: A Nortel Networks proprietary MIB is included on the Nortel Networks CD-ROM. Click on the file named CesTraps.mib to load the MIB. See “Contivity Extranet Switch MIB Support” for a description of CesTraps.mib.

You can view the Health Check screen for the results of SNMP Traps.

Figure 140 SNMP

SNMP-GET HOSTS

Enable	Host Name or IP Address	Community Name	Status
1 ☐			
2 ☐			
3 ☐			

TRAP HOSTS

Enable	Host Name or IP Address	Community Name	Status
1 ☐			
2 ☐			
3 ☐			

TRAP CONFIGURATION

Enable	Description	Status	Interval	Action
☐	Traps on health warnings		00:05:00	
☐	Traps on health alerts		00:02:00	
☐	Generate periodic heartbeat		01:00:00	
☐	Traps on hardware warnings and alerts		00:02:00	
☐	Trap on intrusions		00:05:00	
☐	Trap on failed login attempts (LoginTrap)		00:05:00	
☐	Generate power up trap		23:59:59	

OK Cancel Trap Settings Refresh

SNMP GET HOSTS

The SNMP Get Hosts portion of the screen is used to designate SNMP management systems that are authorized to send SNMP Get requests to the Switch. The Switch ignores Get requests that come from all other systems.

Enable

Click to authorize the specified SNMP management system to send SNMP Gets.

Host Name or IP Address

Enter the Host Name or IP address for the SNMP management station that sends the SNMP Gets.

Community Name

Enter the SNMP Community Name. SNMP Communities serve as an Authentication scheme to enable a network device to validate SNMP Traps from the Switch.

Status

Operational indicates that the Switch can talk to the SNMP Get Host, while **Error** indicates the Switch is unable to make a connection to the host.

TRAP HOSTS

The Trap Hosts portion of the screen is used to designate those systems to which SNMP trap messages can be sent.

Enable

Click to Enable the Trap Host to receive SNMP Traps.

Host Name or IP Address

Enter the Host Name or IP address for the SNMP Trap hosts that receives the SNMP Traps.

Community Name

Enter the SNMP Community Name. SNMP Communities serve as an Authentication scheme to enable a network device to validate SNMP Traps from the Switch.

Status

Operational indicates that the Switch can talk to the Trap Host, while Error indicates the Switch is unable to make a connection to the host.



Note: Certain MIB browsers (for example, SNMPC) only accept traps from a machine that it can also do SNMP Gets from. If your MIB browser has this requirement, you must specify the host name or IP address in both the SNMP Get Hosts and Trap Hosts portions of the SNMP screen. Check your MIB browser documentation for requirements.

TRAP CONFIGURATION

Enable

Click to Enable the specific group of SNMP Traps. When enabled, the Switch checks the status at the assigned Interval and send traps to the specified SNMP host servers.

Description

This field lists the conditions that generate SNMP Traps. A check for the trap condition is made at the indicated trap interval. If the trap condition occurs when the check is made, an SNMP Trap is generated. Traps continue to be sent until the condition state clears.

Traps on health

These traps indicate that a hardware or software component has gone into a warning state. The default interval is 00:05:00 (5 minutes).

Trap on health alerts

These traps indicate that a hardware or software component has gone into an alert state. An alert is more severe than a warning. The default interval is 00:02:00 (two minutes).

Generate periodic heartbeat

This trap indicates that the Switch is active. This trap is a good test mechanism to verify that the Switch is on. The default interval is 01:00:00 (1 hour).

Trap on hardware warnings and alerts

These traps indicate that a warning or alert on any of the following hardware components has occurred. Refer to the discussion on Trap Settings for additional information on specific traps. The default interval for these traps is 00:02:00 (2 minutes).

- Intrusion (the top cover has been opened)
- LAN or WAN interfaces
- One of the dual power supplies has failed
- Either the critical or normal temperature is out of range
- One of the voltage indicators is out of range
- A cooling fan is not working properly
- System memory is low
- Disk space is low

Trap on intrusions

This trap indicates that someone has attempted to send an excessive amount of unauthorized packets through the public interface. The trap contains the user ID and the source and destination IP addresses.

Trap on failed login attempts

This trap indicates that someone has attempted to log on to the Switch and failed. The trap contains the user ID and the source and destination IP addresses.

Generate power Up trap

This trap indicates that the Switch has gone through a power-up sequence. This trap occurs only once (the default interval, 23:59:59 is ignored).

Status

Shows when a trap was last executed, along with the timestamp. If a trap is generated, a brief description appears.

Interval

Provides a time interval after which the Switch checks for new SNMP Trap conditions.

Action

If a trap has occurred, click on the Details button in the Action column to view information about the trap. The Details output includes the System Name, Date and Time, System Uptime, and possibly other information (for example, LAN on Slot *n* Interface *n*).

VRRP

Click to enable VRRP SNMP traps.

OSPF

Click to enable OSPF SNMP traps.

SNMP Authentication

Click to enable SNMP Authentication traps.

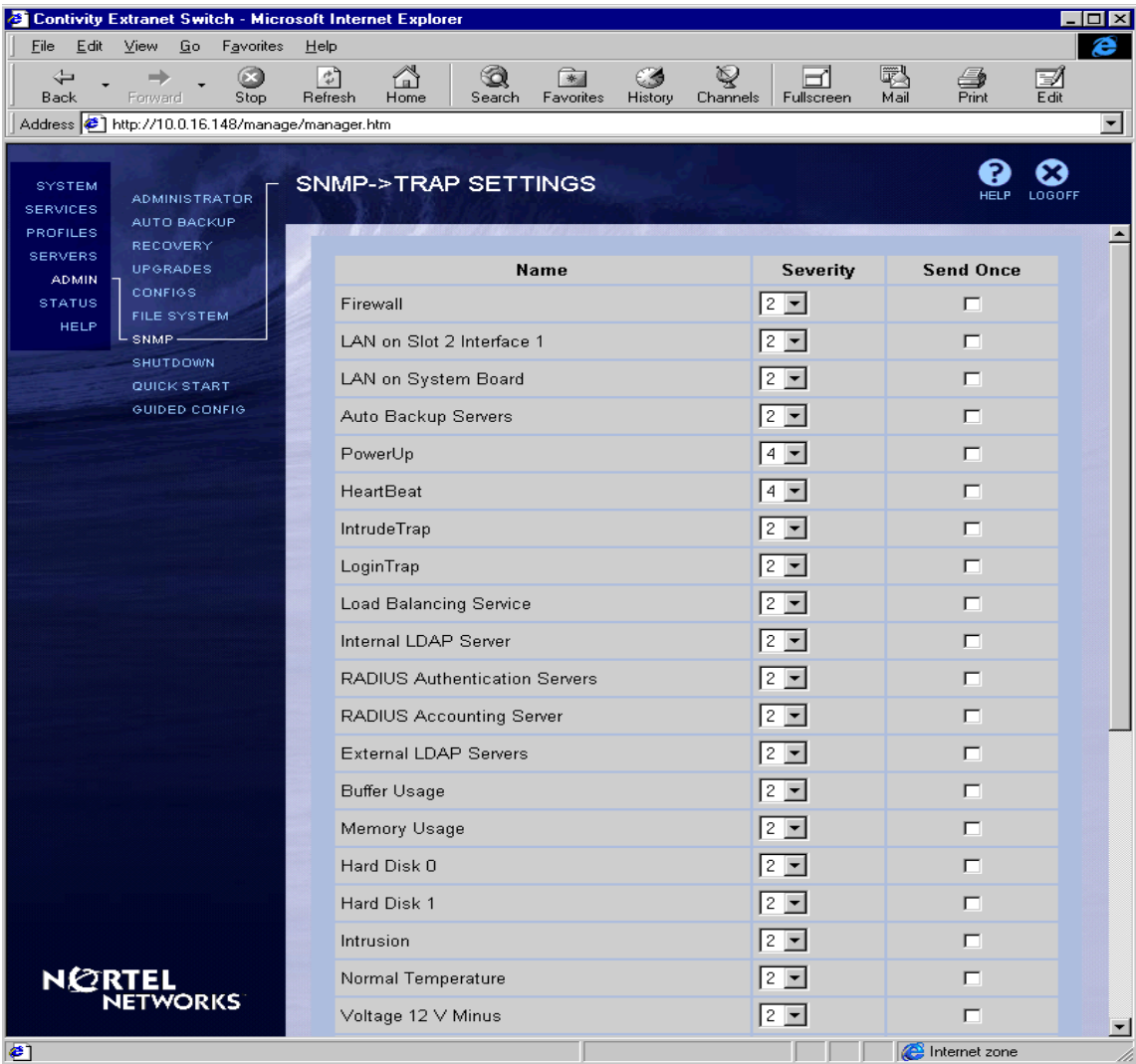
Trap Settings

Click on this button to go to the Trap Settings screen.

SNMP Trap Settings

The SNMP Trap Settings screen (Admin→SNMP→Trap Settings) allows you to specify the level of severity that is reported for the trap. You can also specify that the trap be sent only once.

Figure 141 SNMP Trap Settings



Note: The results of many of the selections you make on the Trap Settings screen are reported on the Health Check screen. Refer to “Alert and Warning Descriptions for Selected Servers” for additional information.

Name

The Name column lists the traps that are available on your Switch. The actual list can vary, depending upon the model of your Switch and your configuration. For example, if your Switch has a single hard disk, the trap that refers to an optional disk (Hard Disk 1) does not appear on your Trap Settings screen.

Firewall

Status of the firewall that is currently enabled on the Switch (either the Contivity Firewall or the Check Point firewall).

LAN on System Board

Current status of LAN Interface 1. The trap is sent only if a problem occurs.

LAN on Slot n Interface n

Current status of Slot n Interface n . The trap is sent only if a problem occurs.

Auto Backup Servers

Current status of the automatic backup servers. The trap is sent only if a problem occurs, for example, if there is no server specified.

PowerUp

Indicates that the Switch was powered up.

HeartBeat

Indicates the status of the heartbeat.

IntrudeTrap

Indicates that excessive unauthorized packets were sent to the Switch.

LoginTrap

Indicates that an attempted login to the Switch failed.

Load Balancing Service

Current status of the load balancing feature. The trap is sent only if a problem occurs. The following table shows possible trap messages and meanings.

Table 23 Load balancing service trap messages

Trap Message	Meaning
Warning: Load Balancing Service: Timed out waiting for response from server	Indicates that Load Balancing is enabled (on the Services→IPSec screen) but the configured server is not responding.

Internal LDAP Server

Current status of the internal LDAP server. The trap is sent only if a problem occurs. The following table shows possible trap messages and meanings.

Table 24 Internal LDAP server trap messages

Trap Message	Meaning
Alert: Internal LDAP Server: Server not running	Server is configured and selected but is not running. This is displayed after a Restore or Backup operation.
Alert: Internal LDAP Server: Server not enabled	Server is running but is not selected
Warning: Internal LDAP Server: Restore in progress	Restore from an LDIF file in progress. LDAP server is selected but is not running. This changes to an Alert (Server not running) condition when the restore is complete
Warning: Internal LDAP Server: Backup in progress	Backup to an LDIF file in progress. LDAP server is selected but is not running. This changes to an Alert (Server not running) condition when the backup is complete.

RADIUS Accounting Server

Current status of the RADIUS Accounting servers. The trap is sent only if a problem occurs. The following table shows possible trap messages and meanings.

Table 25 RADIUS accounting server trap messages

Trap Message	Meaning
Alert: RADIUS Accounting Server: Error	Server has an error condition.

RADIUS Authentication Servers

Current status of the RADIUS authentication servers. The following table shows possible trap messages and meanings.

Table 26 RADIUS authentication server trap messages

Trap Message	Meaning
Alert: RADIUS Authentication Servers: Error	All enabled servers have errors
Warning: RADIUS Authentication Servers: Configured	The first server that was enabled is available but has not been contacted for authentication yet. At least one other enabled server has an error.
Warning: RADIUS Authentication Servers: Operational	The first server that was enabled is operational and has been used for authentication. At least one other enabled server has an error
Warning: RADIUS Authentication Servers: Error	The first server that was enabled has an error. At least one other enabled server is available

External LDAP Servers

Current status of the External LDAP servers. The trap is sent only if a problem occurs. The following table shows possible trap messages and meanings.

Table 27 External LDAP servers trap messages

Trap Message	Meaning
Alert: External LDAP Servers: Server is down	No servers are running and no servers are selected.
Alert: External LDAP Servers: Server not enabled	All servers are running but none have been selected
Warning: External LDAP Servers: Server is down	At least one server is not running and is not selected.
Warning: External LDAP Servers: Server not enabled	At least one server is running but it is not selected.

Buffer Usage

Indicates the status of the buffer. A warning is sent if more than 75 percent of the buffer is being used. If usage exceeds 87.5 percent, an Alert is sent.

Memory Usage

Indicates the status of the system memory. A Warning is sent if more than 75 percent of memory is being used. An Alert is sent if more then 87.5 percent of the memory is being used.

Hard Disk 0

Indicates the status of the hard disk. A Warning is sent if the disk is more than 75 percent full. An Alert is sent if more then 87.5 percent of the disk is full.

Hard Disk 1

This trap appears only if the Switch has a second hard disk, and indicates the status of the second disk. A Warning is sent if the disk is more than 75 percent full. An Alert is sent if more then 87.5 percent of the disk is full.

Dual Power Supply

This trap appears only if the Switch has a dual power supply, and indicates the state the dual power supply.

Table 28 Dual power supply trap message

Trap Message	Meaning
Alert: Dual Power Supply: Redundant supply faulted	On systems with dual power supplies, one of the power supplies is not working. Notes: The switch continues to operate with a single power supply. However you should replace the faulty power supply as soon as possible

Intrusion

Indicates that the Switch cover is off. Sensors in the Switch make this determination.

Table 29 Intrusion trap message

Trap Message	Meaning
Alert: Intrusion: Box has been opened	The cover of the switch has been opened or is being opened, indicating a possible security intrusion. Notes: The switch continues to operate while the box is opened. Check to ensure that unauthorized access has not occurred.

Critical Temperature

Indicates the critical temperature state of the Switch. If this temperature reaches an Alert condition, you should immediately shut down the Switch to prevent any damage.

Table 30 Critical temperature trap message

Trap Message	Meaning
Alert: Critical Temperature: Critical temperature out of range	The switch is running at a critically high temperature above its rated normal operating temperature. This indicates a serious problem -- you should shut down the switch immediately. Notes: Component failure may have already occurred. Contact your Nortel Networks representative if you cannot determine the cause of the excessive temperature

Normal Temperature

The normal temperature state of the Switch. An Alert condition indicates that the Switch has exceeded its normal operating range (0°C to 55°C).

Table 31 Normal temperature trap message

Trap Message	Meaning
Alert: Normal Temperature: Normal temperature out of range	The switch is running above its rated normal operating temperature. Notes: This can occur if the switch fan is not working properly or if there is a high ambient temperature. Continued operation of the switch at excessive temperature can result in performance degradation and component failure. Do not wait for a Critical Temperature Trap, as it is not supported on all switch models

Voltage 12 V Minus

Indicates the state of the -12 voltage. The following table shows voltage-related trap messages.

Table 32 Voltage trap messages

Trap Messages	Meaning
Alert: Voltage <i>nnn</i> : Voltage out of range where: <i>nnn</i> is the voltage, for example, 3.3 V Plus	The supplied voltage to the switch is not within the specified range. This indicates a serious problem and should be checked immediately by a Nortel Networks representative. Notes: Improper voltage input can cause erratic switch operation. Not all switch models support traps for all voltages

Voltage 12 V Plus

Indicates the state of the +12 voltage.

Voltage 2.5 VB

Indicates the state of the 2.5 voltage on the auxiliary processor.

Voltage 2.5 VA

Indicates the state of the 2.5 voltage on the main processor

Voltage 3.3 V Plus

Indicates the state of the +3.3 voltage.

Voltage 5 V Minus

Indicates the state of the -5 voltage.

Voltage 5 V Plus

Indicates the state of the +5 voltage.

Chassis Fan 2

Current status of the second chassis fan. If you have an Alert, check to see if the fan is dirty or clogged. This trap is displayed only if the Switch has the second chassis fan.

Table 33 Chassis Fan 2 trap message

Trap Messages	Meaning
Alert: Chassis Fan 2: Fan not functioning	The second chassis fan is running either below the specified speed or is not running at all. Notes: A service technician must check the fan as soon as possible. If the fan is not working correctly, overheating of the switch and possible component failure can result.

Chassis Fan

Current status of the chassis fan. If you have an Alert, check to see if the fan is dirty or clogged.

Table 34 Chassis fan trap message

Trap Messages	Meaning
Alert: Chassis Fan: Fan not functioning	The chassis fan is running either below the specified speed or is not running at all. Notes: A service technician must check the fan as soon as possible. If the fan is not working correctly, overheating of the switch and possible component failure can result.

CPU Two Fan

Current status of the second CPU fan. If you have an Alert, check to see if the fan is operational. This trap is displayed only if the Switch has the second CPU fan.

Table 35 CPU two fan trap messages

Trap Messages	Meaning
Alert: CPU Two Fan: Fan not functioning	The fan on the auxiliary processor is running either below the specified speed or is not running at all. Notes: This trap can only be sent by systems which contain an actual fan on the auxiliary CPU. If the fan is not working correctly, it must be fixed as soon as possible or damage may result to the processor as well as to the switch.

CPU One Fan

Current status of the primary CPU fan. If you have an Alert, check to see if the fan is operational.

Table 36 CPU one fan trap messages

Trap Messages	Meaning
Alert: CPU One Fan: Fan not functioning	The fan on the primary processor is running either below the specified speed or is not running at all. Notes: This trap can only be sent by systems which contain an actual fan on the primary CPU. If the fan is not working correctly, it must be fixed as soon as possible or damage may result to the processor as well as to the switch.

CPU 2

Current status of the second CPU. This trap is displayed only if the Switch has two CPUs.

Table 37 CPU 2 trap message

Trap Message	Meaning
Alert: CPU 2: Program load failed	These traps are only sent from a Switch with multiple CPUs and indicate that the application CPU is not functioning correctly. Notes: The switch sounds an alarm and the networking performance is degraded. The switch continues to function without the application processor. Reboot the switch to correct the situation. If the problem continues, contact your Nortel Networks support representative
Alert: CPU 2: Bootup did not complete	
Alert: CPU 2: Communication los	
Alert: CPU 2: Failed. Reason unknown	

SNMP Servers

Current status of the SNMP servers. The status is either Operational or Error.

IP Address Pool

The status of the IP Address Pool. An Alert status indicates that there are no addresses available.

FIPS

Current status of FIPS mode.

Table 38 FIPS trap messages

Trap Message	Meaning
OK: FIPS disabled	FIPS mode is currently disabled on the Switch
OK: FIPS enabled and power-up test in progress	FIPS mode is enabled and the Switch has been rebooted and is running the power-up tests
OK: FIPS enabled and all tests have passed	FIPS mode is enabled, the Switch has finished rebooting, and has successfully completed the power-up tests.
Warning: FIPS: Random generator test failed	During the FIPS power-up testing, the random generator test failed.
Warning: FIPS: DESMAC check on executables failed	During the FIPS power-up testing, DESMAC check on executables failed.
Warning: FIPS: DES KAT test failed	During the FIPS power-up testing, the DES KAT test failed.
Warning: FIPS: SHA1 self test failed	During the FIPS power-up testing, the SHA1 self test failed
Warning: FIPS disabled due to HW accelerator presen	FIPS is disabled because your Switch has a hardware accelerator card installed.
Alert: FIPS status not known	The Switch is unable to determine the status of FIPS mode.

DNS Servers

Current status of the DNS servers. The following table shows possible trap messages and meanings.

Table 39 DNS servers trap messages

Trap Messages	Meaning
Alert: DNS Servers: Error	None of the configured servers are operational
Warning: DNS Servers: Operational	At least one server is operating properly but another server has errors.

Severity

Click the drop-down list box to select the level of severity that is reported for the trap. The default severity is a value of 2. In most cases, the default is appropriate for the trap. However, you might want to change the severity value to highlight the reporting of a trap. For example, if you want to closely monitor the status of your hard disk, you might assign a severity value of 1 to the Hard Disk 0 trap.

The following table shows the severity choices and their impact on the Switch performance.

Table 40 Severity Level Meanings

Severity	Meaning
1	Fatal, critical condition; severely impacts performance.
2	Major condition; results in poor performance.
3	Minor condition; performance is within specifications but should be monitored.
4	Significant informational event; normal performance.
5	Event of no operational value.
R	Reverses Severity 1, 2, and 3 conditions; returns performance to normal. This code is for future use.

Send Once

This selection takes precedence over the Interval setting on the SNMP screen. Click to specify that if the event occurs, it is trapped only once. Otherwise the trap is repeated using the time interval specified on the SNMP screen. The PowerUp trap is an example of a send once event.

System Shutdown

The Admin→Shutdown screen allows you to gracefully turn off the Switch. The Shutdown options allow you to Shutdown immediately, to wait until current users are logged off, or to wait until a designated time. A graceful shutdown safely terminates connections so that no data is lost, compared with a spontaneous loss of power, for example.

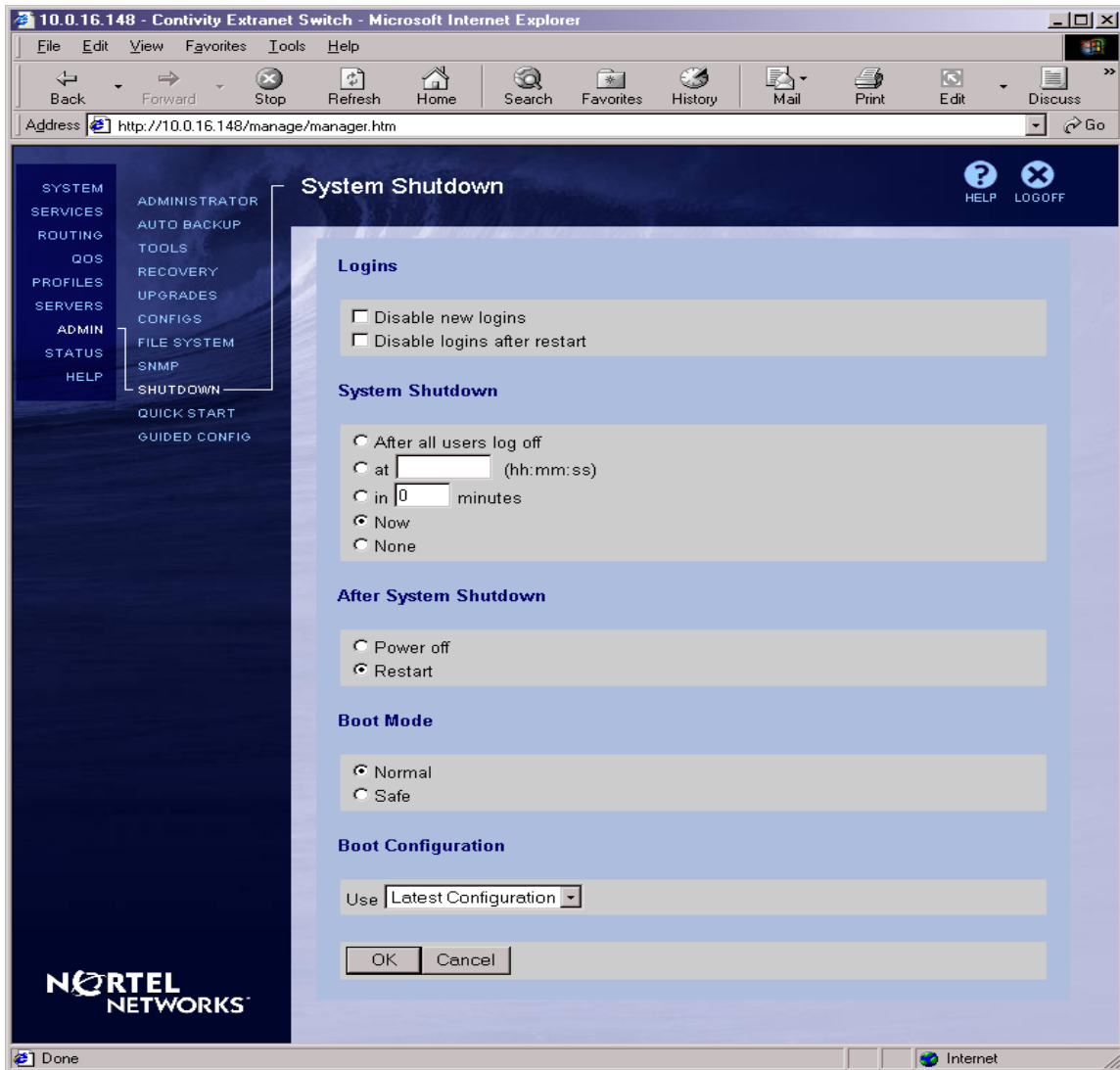
Additionally, you can select whether to power off or restart after Shutdown, and also choose the configuration file to use upon restarting. To allow you to conduct an orderly Shutdown, you can disable new logins, and you can disable logins after the Shutdown to perform system maintenance.

You should always use the System Shutdown screen to shut down the system rather than the Power or Reset buttons on the back of the Switch. This ensures the integrity of your file system.



Note: After performing a System Shutdown, click the Reload/Refresh button to see the latest Switch information.

Figure 142 System Shutdown



Caution: When a System Shutdown has started, do not reset or power down the Switch; doing so might cause you to lose data or might render the Switch inoperable.

Logins

Disable New Logins

Click to prevent new remote access logins before shutting down. Disabling New Logins prevents the need to log off new users when you power down the system.

Disable Logins After Restart

Click to prevent remote Logins After Restarting the system. For example, you might select this option when performing system maintenance. After the system restarts, the Disable New Logins option is selected. After completing maintenance tasks, you should deselect Disable New Logins to allow normal logins.



Note: Administrators can access the Switch via Web management independent of the Login control selection.

System Shutdown

To Shutdown, you must select a System Shutdown option other than None, which is the default.

After All Users Log Off

Click to shut down the system After All remote access Users have Logged Off. Administrators logged into the system via HTTP must also be logged off.

At

Click and assign a specific time to shut down the system as represented by a 24-hour clock (hh:mm:ss); for example, you can shut down the system at 16:50:00.

In *n* Minutes

Enter a specific number of Minutes after which the system shuts down. The possible range is 1 to 1440 (24 hours); default is 1 minute.

Now

Safely shuts down the system immediately by terminating all sessions and closing connections to servers.

None

Do not shut down the system. If there is a previously configured shutdown pending, you must click on the Cancel Pending Shutdown button at the top of the screen. This cancels the pending shutdown and automatically selects the None option.

After System Shutdown

Power Off

Power Off the Switch After the System Shutdown occurs.

Restart

Restart the Switch After the System Shutdown occurs.

Boot Mode

Select the mode that you want to use when rebooting the Switch, either Normal mode or Safe mode.

Boot Configuration

Use

Click the drop-down list box to view the available Configuration Files. To change the configuration files that appear in this list, use the Current System Configuration screen. Select the configuration file that you want the Switch to boot from when restarting.

Note that if you choose a new Boot Configuration option, then you must also choose a System Shutdown option to indicate when the System shuts down and subsequently loads the new Boot Configuration file.

Reboot From Drive

/ide0/ (primary)

Click to select the hard disk drive */ide0/ (primary)* from which you want to boot the Switch.

/ide1/ (secondary)

Click to select the hard disk drive */ide1/ (secondary)* from which you want to boot the Switch.

Cancel Pending Shutdown

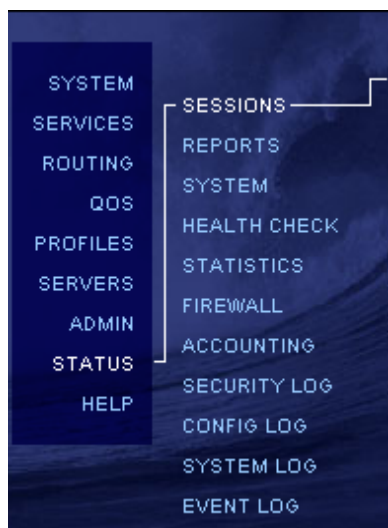
When a shutdown is pending, the Cancel a Pending Shutdown button is available. Use this button to stop the shutdown or, alternatively, click None under the System Shutdown area of the screen.

Chapter 8

Status

This section describes the System Status screens. The System Status screens allow you to see, from the Web interface, who is logged on, their traffic demands, and a summary of the Switch hardware configuration, including available memory and disk space.

Figure 143 Status Menu



Active Sessions

The Active Sessions screen allows you to see which users are tunneled into the Switch, when they logged in, and the number of bytes and packets they have transmitted or received.

Additionally, you can choose to see selected session details and you can even log off users.

Figure 144 Active Sessions

Display
All Sessions

Summary

	Branch Office	End User IPSEC	End User PPTP	End User L2TP	End User L2F	Admin	Total
Current Sessions	0	0	0	0	0	3	3
Peak Sessions for 04/01	N/A	0	0	0	0	4	4
Total Sessions Since Boot	N/A	0	0	0	0	3	3

Current Branch Office Sessions

Connection	Type	UserID	Address	Start	Kbytes	Packets	Action
------------	------	--------	---------	-------	--------	---------	--------

Current End User Sessions

User	Type	UserID	IP Address Assigned Public	IPX Address	Start	Kbytes	Packets	Links	Action
admin	Admin	admin	132.245.250.103		04/01/1999 18:04:23				Logoff
admin	Admin	admin	132.245.250.103		04/01/1999 18:01:25				Logoff
admin	Admin	admin	132.245.250.53		04/01/1999 17:54:40				Logoff

Refresh

Logoff all non-Admin Users

Logoff all Branch Office Connections

Display

Click the drop-down list box to select one of the following Active Sessions views:

- End User Sessions

- Branch Office Sessions
- All sessions (default)

Summary

The Summary table shows statistics for the number of sessions on the Switch, including the current number of sessions, the peak number of sessions, and the total number of sessions since the Switch was last booted.

Current Sessions

The current number of sessions.

Peak Sessions for Date

The maximum number of sessions for the cited date.

Total Sessions Since Boot

The total number of sessions since the system was restarted.

Current Branch Office Sessions

Shows the number of Branch Office connections, including the gateway, IP address, start time, number of Kilobytes, and total packets sent through a connection.

Refer to the Current End User Sessions section for most of the Current Branch Office Sessions field descriptions, as they are the same.

Connection

Shows the name of the Connection, either an IP address or a DNS name.

Current End User Sessions

Shows the current end user connections to the Switch, including the user name, type, User ID, IP address assigned, the IPX address, start time, number of Kilobytes, total packets sent through a connection, and links.

User

Shows the User's full name; for example, Madison Lee.

Type

Shows the account Type, any of the four tunnel types (IPsec, PPTP, L2TP, L2F) or Admin.

User ID

Shows the User's account ID; for example, mlee.

IP Address Assigned/Public

Shows the IP Address Assigned by the Switch (the inner address), and the public IP Address of the client device (possibly assigned by the ISP) that is connected to the Switch.

IPX Address

Shows the inner IPX Address of the client device that is connected to the Switch.

Start

Shows the session Start date and time using a 24-hour clock (in the format hh:mm:ss). For example, 6/5/1999 21:18:47.

Kbytes

Shows the number of Kilobytes of traffic transmitted In to the corporate network and Out of the corporate network. (Not applicable to Administrator's sessions.)

Packets

Shows the number of Packets going into the corporation and going out of the enterprise's intranet. (Not applicable to Administrator sessions.)

Links

Shows the number of PPP links associated with this session.

Action*Log Off*

Click to log off the associated user immediately, including Administrators. The Log Off button appears only if you have the proper Administrator rights.

Details

Click to view Details such as the group the user belongs to, account type, number of active sessions, and numerous IP session counters. This option is not applicable to Administrator sessions.

Log Off

Click to log off all non-administrative users immediately. This logs off all tunneled users so that the administrator can perform maintenance.

Active Sessions Details

This screen provides Active Session Details for specific users, including User Name and Group, number and type of accounts, number of active sessions and many IP session-specific details.

Figure 145 Partial Active Sessions Details

The screenshot shows a window titled "Active Sessions Details" with a "Close" and "Refresh" button. The main content area displays session statistics for the network 10.15.x.x net. The date is 04/01/1999 and the time is 19:25:52. The session details include:

```

Name: 10.15.x.x net
Account Type: L2TP
Number of Sessions: 1
Session Subnet: 0.0.0.0 - 0.0.0.0
Session Start Date: 04/01/1999
Session Start Time: 09:06:45
Session Total KBytes In: 2173
Session Total KBytes Out: 2173
Session Total Packets In: 37094
Session Total Packets Out: 37098
Session Filter Drops In: 0
Session Filter Drops Out: 0
Session Total QoSRandom Drops In: 0
Session QoSRandom Drops Out: 0
Session QoSForced Drops In: 0
Session Total QoSForced Drops Out: 0
Session IpHdr Drops In: 0
Session IpHdr Drops Out: 0
Session IpFrag In: 0
Session IpFrag Out: 0
Session IpFrag Drops In: 0
Session IpFrag Drops Out: 0

```

Below the session details, there is a section for "Packets Out: Total/QoS Dropped/Flow Control Dropped" and "On cpu: 1". The ICP section shows the state as "Opened" and various statistics for Conf, Term, and Code messages. The PAP Statistics section shows the Server State as "Closed" and Client State as "Closed". The Auth section shows the Auth-Req's out: 0 / 0 / 0, Auth-Ack's out: 0 / 0 / 0, and Auth-Nak's out: 0 / 0 / 0. The CHAP derivative is not recognized, and the Server State is "Open" and Client State is "Closed".

The following table provides descriptions of active sessions.

Table 41 Descriptions of Active Session Details

Listing	Description
User Name	Current user's name
Group	Group with which the current user is associated
Number of Accounts	Number of accounts that are currently active
Account Type	Type of the account
Account Userid	User ID for this account
Number of Active Sessions	Number of sessions that are currently active
Session IP Address	Session inner IP address
Session Start Date	Date the session started
Session Start Time	Time the session started
Session Kbytes In	Kilobytes that are transmitted into the Switch
Session Kbytes Out	Kilobytes that are transmitted out of the Switch
Session Packets In	Packets that are transmitted into the Switch
Session Packets Out	Packets that are transmitted out of the Switch
Session IpFrag Drops In	Packets going into the enterprise network that are dropped if the rest of the fragment does not get there in time
Session IpHdr Drops In	Packets going into the enterprise network that are dropped whenever there is an error in the IP header
Session Local Interface Filter Drops In	Packets destined to a physical interface that are dropped due to lack of authorization access
Session Local System Filter Drops In	Packets destined to a LAN management address but are dropped due to lack of authorization access
Session QosRandom Drops Out	Packets dropped as part of Random Early Detection (RED) congestion
Session Routing Filter Drops In	Packets filtered because no access rights are permitted to the resources specified by the designated filters
Session Source Address Drops In	Packets that are dropped due to a source address access conflict
Session Local Interface Filter Drops Out	Packets coming from a physical interface that are dropped due to lack of authorization access
Session Local System Filter Drops Out	Packets coming from a Switch management address that are dropped due to lack of authorization access

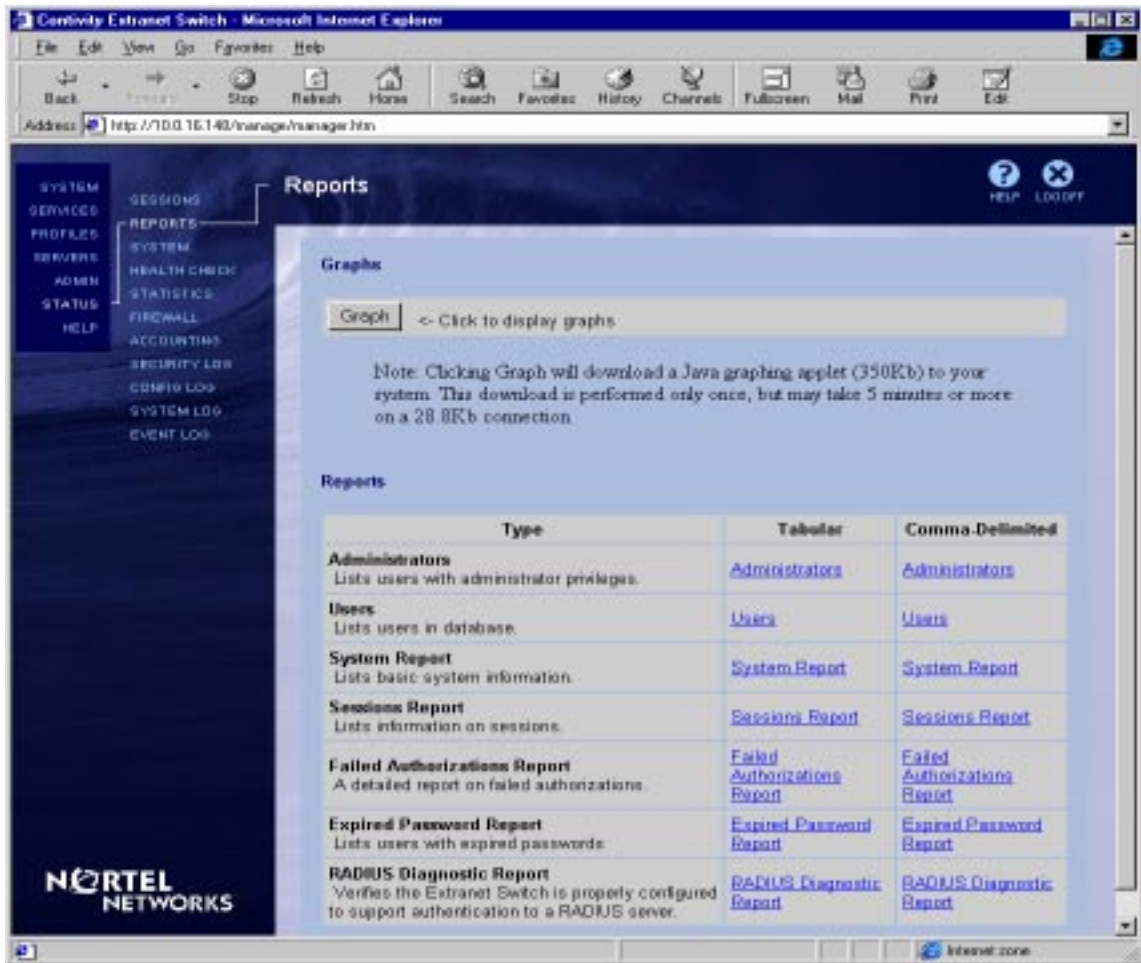
Table 41 Descriptions of Active Session Details

Session QosForced Drops In	Packets dropped because the peer could not establish a quality of service session
Session Routing Filter Drops Out	Packets filtered because no access rights are permitted to the resources specified by the designated filters
Session IpFrag In	Incoming IP packets that are fragmented
Session IpFrag Out	Outgoing IP packets that are fragmented

Status Reports

The Status Reports screen allows you to view system and performance data in text or graphical format. You can generate current or historical graphs of valuable system data. The Reports feature provides a comprehensive screen or down-loadable reports on user activity.

Figure 146 Status Reports



Graph

Clicking Graph causes a Java graphing applet to be loaded to your browser. When you are there, you can choose between graph types and time features. Click to access the graphical package.

The first time you click Graphs, it can take a few minutes for the graphing package to download over a dial-in line. Thereafter, it is cached and appears quickly.

Reports

You can view reports for Administrators or Users. These reports can be accessed in an on-screen tabular format and they can be put into a comma-delimited format for export into a spreadsheet or database.

Type

You can view reports for the following types. The amount of detail in the reports depends on your access rights, which are set in the Admin Rights area on the Profile→Users: Edit screen.

Administrators

You must have Manage Switch rights to view these reports. The report lists users with administrator privileges, including name, group, and Switch or users privileges.

Users

Lists users and the system database groups they are in. You can also generate details of user accounts and user IDs. If you only have Manage User rights, the report is limited to groups that you are allowed to manage.

System Report

You must have Manage Switch rights to view these reports. The report lists basic system information, including configuration, type, services, hardware, and interfaces.

Sessions Report

Lists session information including, model, date, average sessions per minute. If you only have Manage User rights, you must be set up to manage the /Base group.

Failed Authorization Report

Lists failed authorization information including, model, date, total, and average sessions per minute. You can also generate details for individual listings. If you only have Manage User rights, you must be set up to manage the /Base group.

Expired Password Report

Lists users with expired passwords. If you only have Manage User rights, the report is limited to groups that you are allowed to manage.

RADIUS Diagnostic Report

You must have Manage Switch rights to view these reports and the reports are limited to groups that you are allowed to manage. The report lists various RADIUS reports that show whether the Switch settings are synchronized with the RADIUS server settings.

On Screen

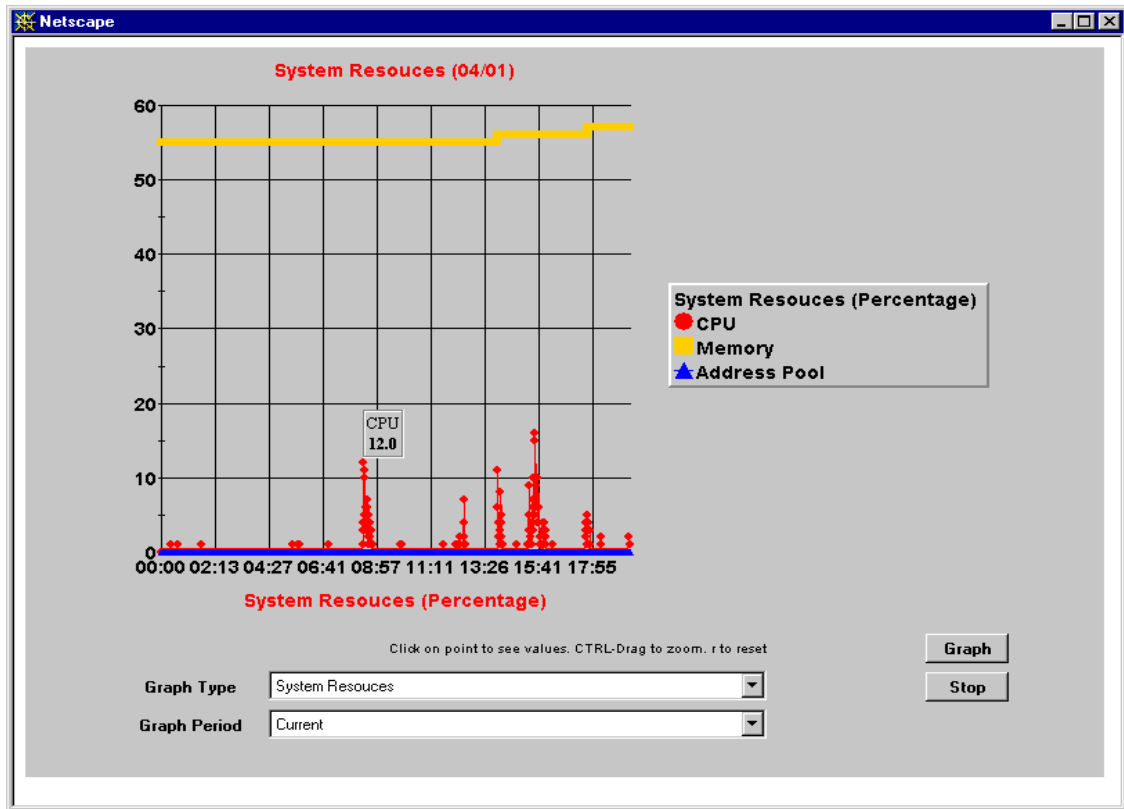
Click the appropriate listing to generate a tabular On Screen report, which you can then print.

Comma-Delimited

Click the appropriate listing to generate the report in a Comma-Delimited format. You can then import this report into a spreadsheet or database.

Graphs

The graphical utility allows you to generate particular types of graphs for specific time periods. For example, you can generate a system resources graph for the current time period.

Figure 147 System Resources Graph

Graph Type

These are the Graph Types that you can generate:

- Bytes In/Out (packets transported by the Switch)
- System Resources
- Dropped Packets
- Failed Authentications
- Packets In/Out
- Sessions

Graph Period

Following are the types of Graph Periods you can generate.

- Current - Displays a per minute average for the entire day up to that point. The graphing package then polls the Switch every minute for the most recent value and appends it to the graph. You can leave Current up and running and it continues to graph throughout the day.
- Historical - Displays summary data for the last 30 days.
- Date - Displays data for the specified date.

Viewing a Single Value

You can display the values represented by any point on the graph by clicking on the exact data point, then clicking again. A dialog box displays the values of the data point.

Zooming in on a Graph Area

To zoom into an interesting portion of the graph, click at a point to the left of the area that you want to enlarge, drag your mouse past the point that you want to enlarge, then release the mouse button. You can repeat this action to further enlarge the viewed area.

Type a lowercase “r” to stop zooming and reset the graph to its original view



Note: Make a rectangle around the full area that you want to view, including all specific data points.

Graph

After making a change to the Graph Type or Graph Period, then click the Graph button to generate a new graph.

Stop

The Stop button, which is available only when graphing current values, stops the browser from updating the graph every minute.

Considerations

Counters

When a graphing counter exceeds the maximum (approximately 4 billion), the counter wraps to zero and the number reported is incorrect until the Switch is restarted.

Upgrading and Graphs

After upgrading the Switch, it can take up to 20 minutes before the system can generate graphs. This delay accounts for the time necessary to collect enough data to begin graphing.

Bytes In and Bytes Out

The graphing application labels the y-axis using scientific notation.

Historical Graph

The Switch must be running at midnight (12:00 a.m.) to generate a historical graph for the day.

Reports

The Reports feature allows you to generate comprehensive reports of users and other important information. You generate Reports in an On Screen tabular format and you can import them into a spreadsheet or database through the Comma-Delimited format.

Tabular Report

You can generate an on screen Users Report in tabular format. It indicates the report type, when it was generated, the model number, and the Domain Name Service (DNS) host name. You can also view the user's group, tunnel type, and User IDs.

Figure 148 Users Report

Report	Users Lists users in database.
Generated	THURSDAY 04/01/1999 19:32:35
Model	NOC4000
DNS Host Name	PDTarget
Page 1	

Next

☐ Includes detailed list of individual user accounts and user IDs

/Base	
	Antoinette, Marie
	Donahue, Peter
	Einstein, Albert
	Fitzgerald, Edmund
	Kostanza, George
	Nessman, Les
	View, View
	Zappa, Frank
/Base/herbn	
/Base/daa	
/Base/dda	
/Base/dea	
/Base/Default Route Test	
	Hannigan, Kerry
/Base/Engineering	
	Bernice, Bernice
	Charles, Charlie
/Base/Field	
/Base/Field/Boston	
/Base/Field/Boston/Ozamonopeia	
/Base/Field/LA	
/Base/Marketing	
/Base/My Company	
/Base/Quick Start Group	

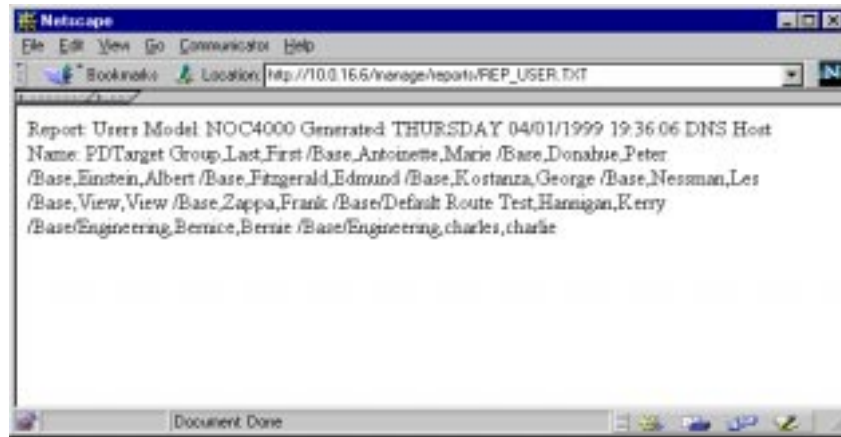
Refresh

End of user list	
Groups	14
Users	11

Comma Delimited Report

You can generate text-based, Comma Delimited reports that can be imported into a spreadsheet or database. The following report includes the same information as the tabular report, but in a Comma Delimited format.

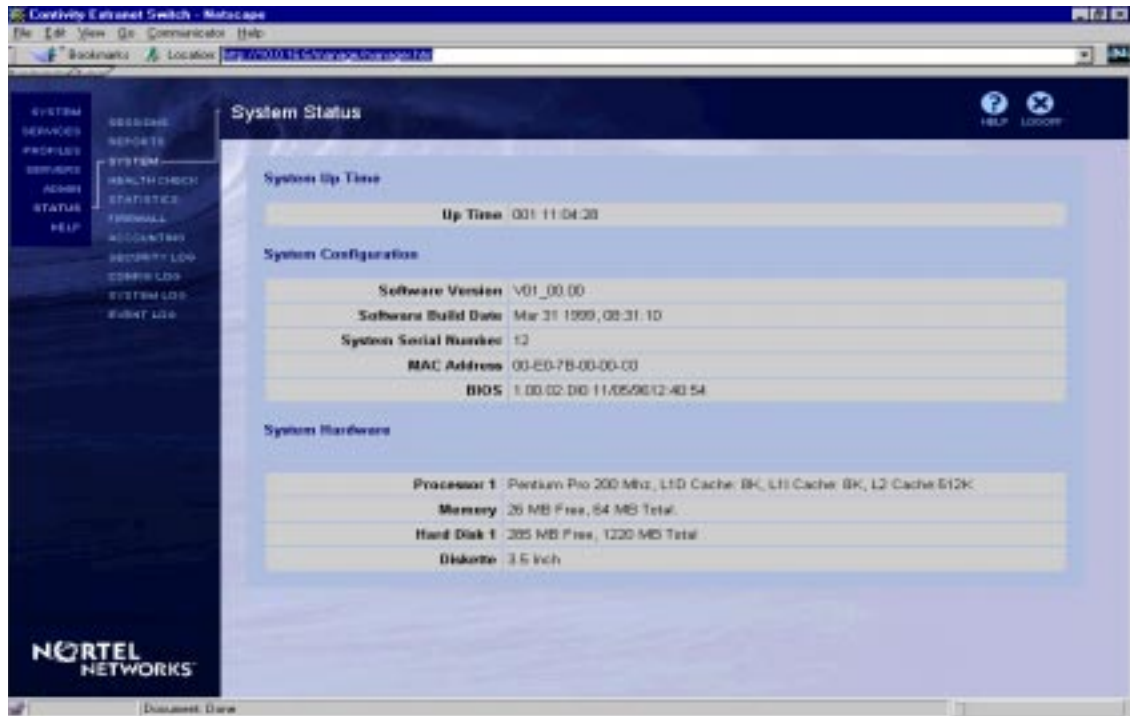
Figure 149 Comma Delimited Report



System Status

The System Status screen shows the Switch's Up Time, software and hardware configurations, along with the current status of key devices. When there is a pending shutdown or an IPX Public Network Address change that requires a reboot, such events are listed at the top of this screen.

Figure 150 System Status



System Up Time

Up Time

Shows the length of time in a 24-hour clock format that the Switch has been running: days (if applicable), hours, minutes, and seconds.

System Configuration

Software Version

The Version of Software currently in use.

Software Build Date

The date and time that the software was built by Nortel Networks.

System Serial Number

The system serial number. This number is unique for each Switch.

MAC Address

The media access control (MAC) address of the logical system management interface.

BIOS

Basic Input/Output System (BIOS) number, date, and time.

System Hardware

Processors 1 and 2

Processors 1 and 2 are Pentium IIs running at 450MHz with 512 KB cache. Only the 4000 series of the switch has dual processors.

Memory

The available memory in the Switch.

Hard Disk 1 and 2

The amount of the hard disk storage that is available on a particular disk, and also the total storage space. In this case, hard disk 1 has 1399 MB available storage out of a total of 2036 MB; thus, 637 MB is being used. Only the 4000 series of the switch has two hard disks.

Diskette

The type of diskette drive (3.5-inch) on the Switch (located behind the front cover or on the front). The diskette drive is not required for normal operation, but is available to restore the system in the unlikely event of a hard disk failure. For instructions on removing the front cover, refer to the switch's *Getting Started Guide*.

Health Check

The Health Check screen provides an overall summary of the current state of the Switch's hardware and software components at a glance.

Figure 151 Health Check

Date: 04/01/1999 Time: 19:41:25

Audible Alarm: ☐ Enable ☒ Disable

Component Name	Status	Description	More Information
LAN on Slot 2 Interface 1	Alert	Device left down	LAN on Slot 2 Interface 1
Disk Redundancy	Alert	Failure	
Voltage 2.5 Vb	Alert	Voltage out of range	
Chassis Fan	Alert	Fan not functioning	
CPU Two Fan	Alert	Fan not functioning	
CPU 2	Alert	Failed. Reason unknown	
Auto Backup Servers	Warning	Server not configured	Automatic Backup
Hard Disk 0	Warning	Utilization exceeds 75% on AdoV	Hard Disk 0
Hard Disk 1	Warning	Device idle / not available	Hard Disk 1
RADIUS Authentication Servers	Warning	Configured	RADIUS Authentication
Firewall	Warning	Firewall disabled	Firewall
Load Balancing Service	Warning	Server not enabled	Load Balancing Service
LAN on System Board	OK	Device left up	LAN Interfaces
Internal LDAP Server	OK	Operational	LDAP Server
RADIUS Accounting Server	OK	Server not enabled	RADIUS Accounting
External LDAP Servers	OK	Server not enabled	LDAP Server
Buffer Usage	OK	Utilization is below 75%	
Memory Usage	OK	Utilization is below 75%	Memory Usage
Dual Power Supply	OK	Operational	
Intrusion	OK	Operational	
Critical Temperature	OK	Operational	
Normal Temperature	OK	Operational	
Voltage 12 V Minus	OK	Operational	
Voltage 12 V Plus	OK	Operational	
Voltage 2.5 Vb	OK	Operational	
Voltage 3.3 V Plus	OK	Operational	
Voltage 5 V Minus	OK	Operational	
Voltage 5 V Plus	OK	Operational	
CPU One Fan	OK	Operational	
SNMP Sensors	OK	Server not enabled	SNMP Traps
IP Address Pool	OK	Operational	IP Address Pool
DNS Servers	OK	Server not configured	DNS Servers

Health Check Support

The following table shows the Health Check values and various models of the Contivity VPN Switch that support them. Gray shading means that the model is supported; white means that it is not supported.* = if a WAN card is installed

Audible Alarm

Enable

Click to Enable the Audible Alarm, which the Switch emits.

Disable

Click to Disable the Audible Alarm, which the Switch emits.

Component Name

This is a brief description of the hardware or software components in the Switch.

Status

The listings appear from top to bottom in order of severity, based on the following possible listings:

- Alert - A red Alert indicates that something is wrong with the current situation and you should attend to the situation as soon as possible.
- Warning - A yellow Warning indicates that there is an impending failure; you should attend to the situation now in order to avoid an Alert condition. A purple Warning indicates that the server is not yet configured.
- Disabled - A yellow Disabled indicates that the device is not enabled on its related configuration screen. For example, the Load Balancing Service would show a Disabled status if you have not checked the Enabled box for Load Balance on the Service→IPsec screen.
- OK - A green OK indicates that everything is currently operating as expected. There are no problems to be concerned with. Note, however, that servers that are not enabled are also listed as OK.

Description

A brief message describes the component state. The section Alert and Warning Descriptions for Selected Servers” lists descriptions for Alert or Warning conditions.

More Information

This column contains a link to the configuration screen associated with the selected component or for a Status→Statistics screen that has related information. This option is left blank when there are no associated screens.

Additional Information for Health Check screen

This section provides additional information for the descriptions that you might receive from the Health Check screen.

Health Check Components

The following table describes the health check components.

Table 42 Health Check Components

Component Name	Description
LAN on Slot <i>n</i> Interface <i>n</i>	Current status of Slot <i>n</i> Interface <i>n</i>
Auto Backup Servers	Current status of the automatic backup servers
SNMP Servers	Current status of the SNMP servers
Load Balancing Service	Current status of the load balancing feature
Firewall	Current status of the Switch's firewall
LAN on System Board	Current status of LAN Interface
Internal LDAP Server	Current status of the internal LDAP server
RADIUS Accounting Server	Current status of the RADIUS Accounting servers
External LDAP Servers	Current status of the External LDAP servers
Buffer Usage	Status of the buffer
Memory Usage	Status of the Switch's system memory
Hard Disk 0	Status of the Switch's hard disk

Table 42 Health Check Components

Dual Power Supply	State the dual power supply
Intrusion	Internal light sensors have determined that the cover is off
Critical Temperature	Critical temperature state of the Switch. If this temperature reaches an Alert condition, the Switch goes into an impending shutdown state to prevent any damage.
Normal Temperature	Normal temperature state of the Switch. If this temperature reaches an Alert condition, then the Switch has exceeded the normal operating range (0°C to 55°C).
Voltage 12 V Minus	State of the Voltage 12 V Minus reading
Voltage 12 V Plus	State of the Voltage 12 V Plus reading
Voltage 2.5 VB	State of the Voltage 2.5 VB reading
Voltage 2.5 VA	State of the Voltage 2.5 VA reading
Voltage 3.3 V Plus	State of the Voltage 3.3 V Plus reading
Voltage 5 V Minus	State of the Voltage 5 V Minus reading
Voltage 5 V Plus	State of the Voltage 5 V Plus reading
Chassis Fan 2	Current status of the LAN/WAN card slot fan. If you have an Alert, check to see if the fan is dirty or clogged.
Chassis Fan	Current status of the LAN/WAN card slot fan. If you have an Alert, check to see if the fan is dirty or clogged.
CPU Two Fan	Current status of the CPU Two Fan. If you have an Alert, check to see if the fan is operational.
CPU One Fan	Current status of the CPU One Fan. If you have an Alert, check to see if the fan is operational.
Disk Redundancy	Current status of the two hard disks.
WAN on Slot <i>n</i> Interface <i>n</i>	Current status of Slot <i>n</i> Interface <i>n</i> .
RADIUS Authentication Servers	Current status of the RADIUS authentication servers
IP Address Pool	Current status of the DHCP Address pool server.
DNS Servers	Current status of the DNS servers
FIPS	Current status of FIPS Mode

Alert and Warning Descriptions for Selected Servers

The use of SNMP traps can provide important status information about your Switch's devices. The following table lists possible Health Check messages that can result when Alert and Warning conditions are produced by SNMP traps. This information is for the following types of servers: RADIUS Servers, LDAP Servers, Load Balancing Servers, and DNS Servers. In some cases, the table also shows descriptions for selected OK conditions.

Table 43 Health Check Messages from SNMP Traps

Status	Description	Comments
<i>RADIUS Accounting Server</i>		
Alert	Error	Server has an error condition.
OK	Server not enabled	No server is available. You must enable the server on the Servers→RADIUS Acct screen.
OK	Configured	No errors.
<i>RADIUS Authentication Server</i>		
Alert	Error	All enabled servers have errors.
Warning	Configured	The first server that was enabled is available but has not been contacted for authentication yet. At least one other enabled server has an error.
Warning	Operational	The first server that was enabled is operational and has been used for authentication. At least one other enabled server has an error.
Warning	Error	The first server that was enabled has an error. At least one other enabled server is available.
OK	Configured	No error conditions.
OK	Operational	No error conditions.

Table 43 Health Check Messages from SNMP Traps

Status	Description	Comments
OK	Server not enabled	No servers available. • Make sure you have enabled RADIUS Authentication on the Servers→RADIUS Auth screen. • Make sure at least one RADIUS server is enabled on the Servers→RADIUS Auth screen.
Internal LDAP Server		
Alert	Server not running	Server is configured and selected but is not running. This is displayed after a Restore or Backup operation.
Alert	Server not enabled	Server is running but is not selected.
Warning	Restore in progress	Restore from an LDIF file in progress. LDAP server is selected but is not running. This changes to an Alert (Server not running) condition when the restore is complete.
Warning	Backup in progress	Backup to an LDIF file in progress. LDAP server is selected but is not running. This changes to an Alert (Server not running) condition when the backup is complete.
OK	Server not enabled	Server is running but is not selected.
OK	Server is down	Server is not running and is not selected.
OK	Operational	Server is running and is selected.
External LDAP Servers		
Alert	Server not enabled	All servers are running but no servers are selected.
Alert	Server is down	No servers are running and no servers are selected.
Warning	Server not enabled	At least one server is running but it is not selected.

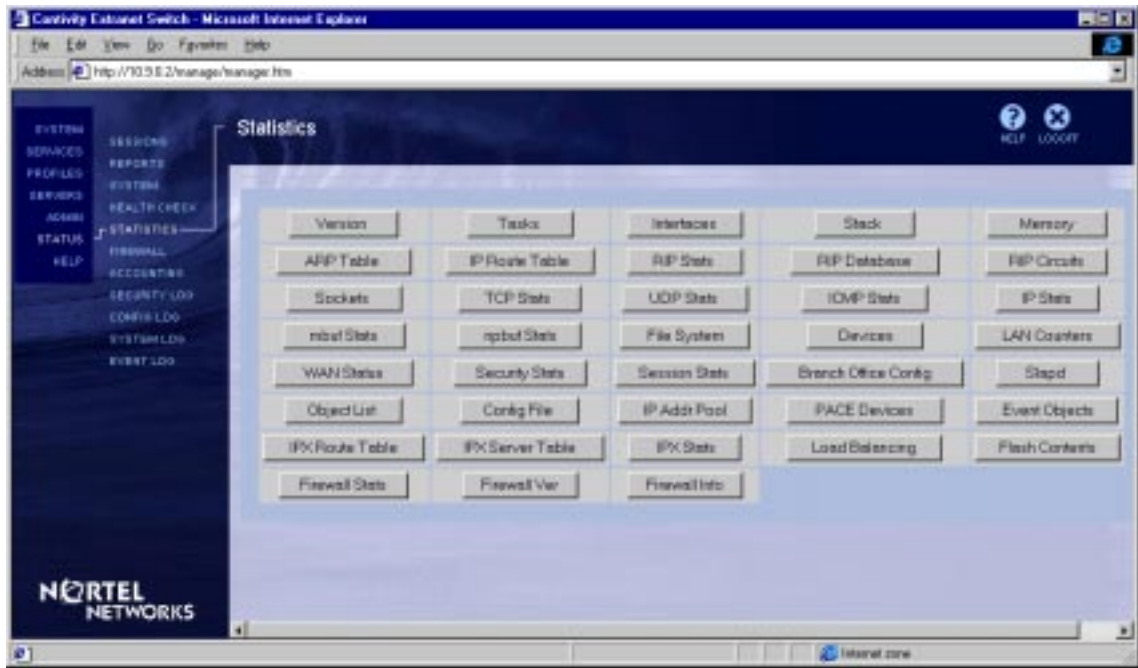
Table 43 Health Check Messages from SNMP Traps

Status	Description	Comments
Warning	Server is down	At least one server is not running and is not selected.
OK	Operational	Server is running and is selected.
<i>Load Balancing Service</i>		
Warning	Timed out waiting for response from server	Load Balancing is enabled and configured, but the server is not responding.
OK	Server not configured	Load Balancing is enabled but no server is configured.
Disabled	Server not enabled	Load Balancing is not enabled on the Services→IPsec screen.
<i>DNS Servers</i>		
Alert	Error	None of the configured servers are operational.
Warning	Operational	At least one server is operating properly but another server has errors.

Statistics

The Statistics screen provides numerous subscreens with a wealth of general and diagnostic information about the Switch hardware, software, and connections. Much of the information is specifically designed for Nortel Networks Customer Support personnel to assist them in diagnosing problems. Some screens, however, such as the LAN Counters, Interfaces, and the WAN Status might provide you with some interesting traffic insights.

Figure 152 Statistics



Buttons

Version

Shows the software version number (for example, V01_05_01.33), creation date, and build level (for example, BL029).

Tasks

Shows the jobs that are currently running within the Switch, including the name, task ID, priority, status, error number, and delay.

Interfaces

Shows the various interface characteristics, including IP and broadcast addresses, subnet masks, the Ethernet address, maximum transfer unit size, packets in and out, multicast packets in and out, and input and output errors.

Stack

Shows the stack characteristics and pointers to the tasks, including name, entry, task ID, and size.

Memory

Shows how memory is being allocated in the Switch, including the current free and allocated memory and the cumulative memory. The information includes status, bytes, blocks, average and maximum block sizes.

ARP Table

Shows the link-level Address Resolution Protocol (ARP) information, including the IP address, destination, gateway, and interface.

Route Table

Shows the internal routing table.

Sockets

Shows the port numbers to which the TCP/IP and UDP protocols are bound.

TCP Stats

Shows the system-wide TCP statistics.

UDP Stats

Shows the system-wide UDP statistics.

ICMP Stats

Shows the system-wide ICMP statistics.

IP Stats

Shows the system-wide IP statistics, including total packets, frames too short and too small, bad header lengths, inbound and outbound fragments, fragments dropped and timed out, packets forwarded, redirects, and reassembled.

Mbuf Stats

Shows the memory for forwarding packets.

File System

Shows the key statistics for each of the Switch's devices, including sectors, bytes per sector, sectors per cluster, and reserved sectors.

Devices

Shows the device drivers associated with the Switch.

LAN Counters

Shows the many LAN transmit and receive counters, all of which are standard for Ethernet devices and are reasonably self-explanatory.

WAN Status

Shows the WAN state variables, configuration values, frame counters, signal values, and the following values.

Table 44 WAN Status Values

IP Fragments Received	Descriptions
Routing Filter Drops	Packets filtered because no access rights are permitted to the resources specified by the designated filters.
Local System Filter Drops	Packets destined for the management interface that are dropped due to lack of authorization access.
Local Interface Filter Drops	Packets destined for a physical interface are dropped due to lack of authorization access.
PAT Drops	Public Address Table (PAT) drops are the number of packets dropped before being authenticated and having a tunnel established.
IP Header Error Drops	Packets with an error in the IP header.

Security Stats

Shows security statistics including total and active sessions by tunnel type and quality of service level, authentication failures, dropped sessions, and so forth.

Slapd

Shows internal LDAP statistics.

Flash Contents

Shows the contents of non-volatile memory.

Object List

This information is for Nortel Networks software engineers only.

Config File

Shows the ASCII contents of the configuration file that is currently in use.

IP Addr Pool

Shows the IP addresses listed in the internal address pool, including the total number and the number of addresses allocated.

PACE Statistics

Shows metrics that are used by the Packet Content Engine, a Nortel Networks internal system.

Event Objects

Shows the internal software objects that are active.

IPX Route Table

Shows the IPX routing table.

IPX Server Table

Shows the IPX server table.

IPX Stats

Shows the IPX statistics.

FIPS

Indicates the status of the Switch's FIPS Certification Mode.

Load Balancing

Shows the traffic load allocation.

Check Point FW-1 Stats

Shows statistics for the integrated Check Point FireWall-1, such as the policy, and rejected and accepted data.

Check Point FW-1 Version

Shows the version and build information for the Check Point FireWall-1

Check Point FW-1 Info

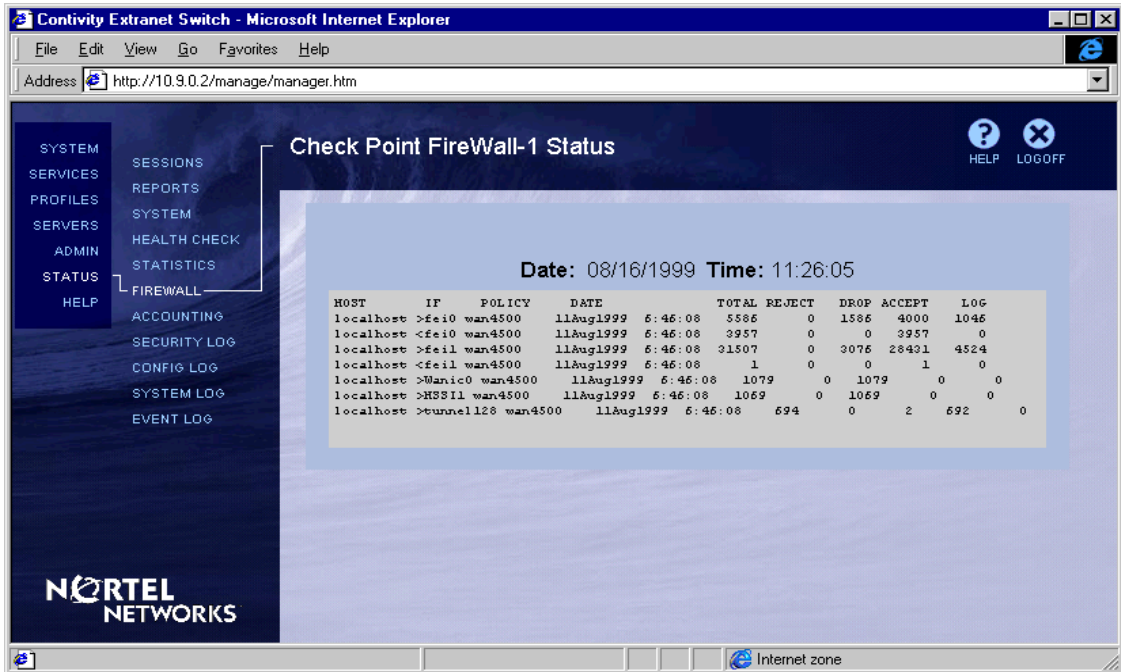
Shows a log file of the Check Point FireWall-1 activity. This information is useful for troubleshooting.

Firewall

The Firewall screen shows the details of the Firewall monitoring session. It is only used for the optional integrated Check Point firewall. This screen provides the same information as the Check Point firewall FW stat -l command.

The message “FW-1 not loaded” is shown if you have specified either the Contivity Firewall or No Firewall on the Services→Firewall screen.

Figure 153 Check Point FireWall-1 Status



Host

The Host is always the “localhost,” which is the Switch that you are currently managing.

Interface

Inbound and outbound packets through the Interface are indicated by the left and right arrows, respectively.

Policy

This is the name of the Policy that is currently in use; default is **Standard**.

Date

This is the Date that the Policy was loaded.

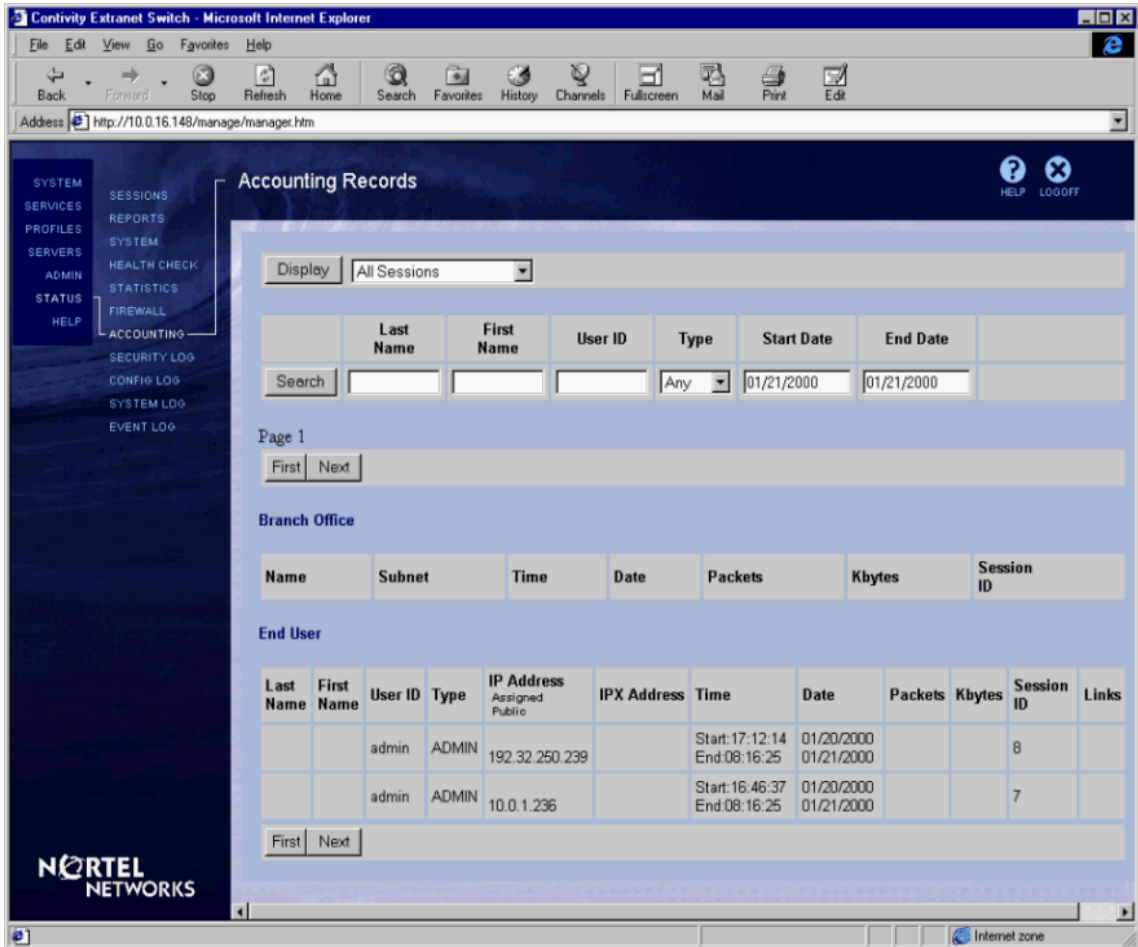
Statistics

The Statistics that are returned provide information about the success or failure of the packet transmissions.

Accounting

Accounting logs User sessions. The Log provides Last and First Names, User ID, Tunnel type, session Start and End Dates, and the number of Packets and Bytes transferred. You can search the log according to most of these fields.

Figure 154 Partial Accounting



Accounting Records

Display

Click to choose between:

- All Sessions
- End User Sessions
- Branch Office Sessions

Search

Enter any combination of the search fields by which you want the log to display, and click Search. You can enter a combination of database field requirements (the search fields can be combined to allow more restrictive searches and narrow the options).

For example, instead of searching for the Last Name OToole only, search for:

Last Name: OToole

End Date: 12/5/97

Type: IPsec

All of the listed criteria must be satisfied. This then displays all activity for anyone named OToole who terminated the IPsec Tunnel Type on 12/5/97.

For Local (nontunneled) sessions certain fields are left blank (for example, Last Name, Packets, Kbytes).

Last Name

Shows the user's last Name.

First Name

Shows the user's first Name.

User ID

Shows the Session User ID.

Group

Allows you to search by user groups name when you screen End User Sessions or by branch office name when you display Branch Office Sessions.

Type

Shows the type of tunnel session used. Possible tunnel type sessions include (refer to the “Tunnel Configuration Overview” section for details):

- IPSec
- PPTP
- L2TP
- L2F

Start and End Dates

Shows the start and end session dates (m/d/y) if the session started and stopped on the same day. If the start and end dates are different (the session starts on Monday and ends Tuesday or later) both dates are displayed.

Session Fields

Some of the session fields are the same as those listed above. Refer to the above references for those descriptions.

Name

Shows the user names.

Subnet

Shows the subnet in which the user’s system resides.

Time

Shows the session start and end times (hh:mm:ss). If the start and end dates are different (the session starts at 18:00 on Monday and ends Tuesday at 03:15) both dates are displayed in the Date field.

Date

Shows the date of the user session.

Packets

The number of Packets transmitted in and out of the Switch during the session.

Kbytes

Shows the number of Kbytes transmitted In to and Out of the Switch during the session. The Switch does not display bytes transmitted in and out for an Administrator session.

Session ID

Shows a system-allocated user Session ID.

User ID

Shows the User ID for the tunnel session.

IP Address

Shows the inner IP Address (Local) and the outer IP Address (Public) of the client devices that are connected to the Switch.

IPX Address

Shows the inner IPX Address (Local) and the outer IP Address (Public) of the client devices that are connected to the Switch.

Links

Shows the number of PPP links associated with this session.

Historical Event Logging

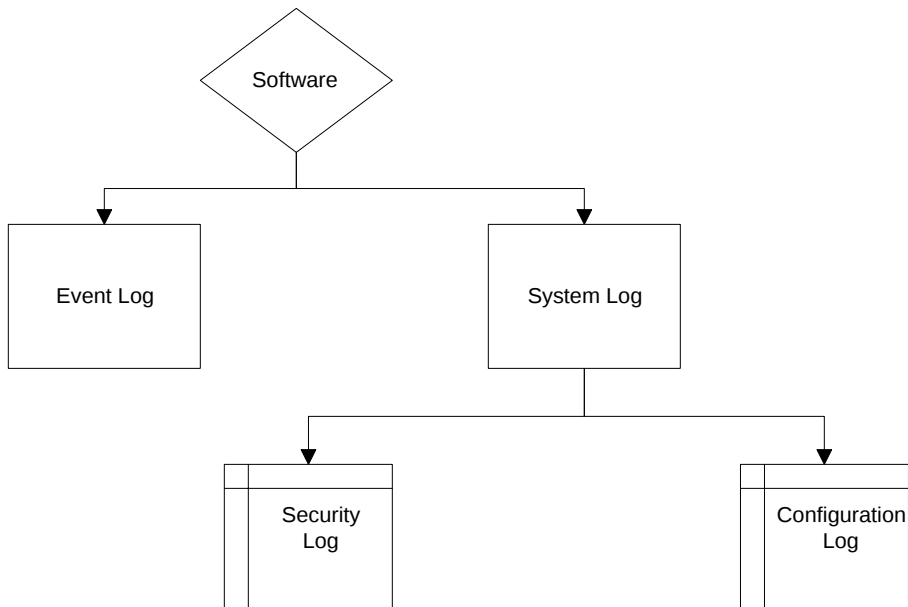
The Switch has several logs that provide different levels of information, including:

- Event Log
- System Log
- Security Log
- Configuration Log

The logs are stored in text files on disk and they indicate what happened, when, and by whom (IP address and user ID).

The Event Log captures real-time logging over a relatively short period of time (for example, the Event Log could wrap its 2000 possible entries in minutes). The System Log captures data over a longer period of time, up to 61 days.

Most events are sent to the Event Log first. Significant events from the Event Log are sent to the System Log. Not all data that is saved by the System Log comes from the Event Log, but that is generally the case. The Switch filters from the System Log security entries for the Security Log and configuration entries for the Configuration Log.

Figure 155 Nortel Networks Logging Scheme

The different Log options allow you to write specific event levels to the log files and view them, including:

- Normal
- Urgent
- Detailed
- All

Common Logging Fields

Introductions to the specific logs appear with each sample log screen. Following are the common field descriptions for the log file screens.

Date

Click to select the Date (mm/dd) of the log you want to view. Then click Display.

This field provides log files for up to the last 61 days.

Display Level

Select the appropriate Log Display level from the following options.

Normal

Normal events are the everyday user and system interactions that allow you to review Switch activity; for example:

- Logins
- Configuration changes
- Scheduled or actual shutdowns

Urgent

Urgent Events are marked with an asterisk in the left column of the log. Urgent Events are those that you want to be aware of immediately and that could potentially pose security or access problems; for example:

- Attempts to login with the wrong password.
- Attempts to gain Administrator Access.

Detailed

Detailed Events are designed specifically for use by Nortel Networks Customer Support personnel to uncover or troubleshoot problems.

All

All Events are also designed specifically for Nortel Networks Customer Support personnel. They include every log message that the system generates, including many details that are not of general interest but might allow Nortel Networks to uncover or troubleshoot problems.

Display

Click to view the log for the selected Date and Level.

Entries

An asterisk indicates an Urgent entry.

A time stamp indicates when (hours:minutes:seconds) the entry was logged.

A task name indicates the software task logging the message. Generally, these tasks refer to the internal system mechanisms and are for Nortel Networks Customer Support personnel only.

The numbers between brackets [01] indicate whether the event is saved to the System Log and also its priority level. If the first number is a one, then the event is sent to the System Log; when it is a zero it is in-memory information. The priority level for the second number is as follows:

0 - Debug

1 - Low

2 - Medium

3 - High

Therefore, the numbers in brackets [12] represent an event that is sent to the System Log and is considered to be of Medium priority.

The task type indicates the actual type of task that was recorded, for example, Security. Task types are often followed by a corresponding task type number.

A brief message describes the entry.

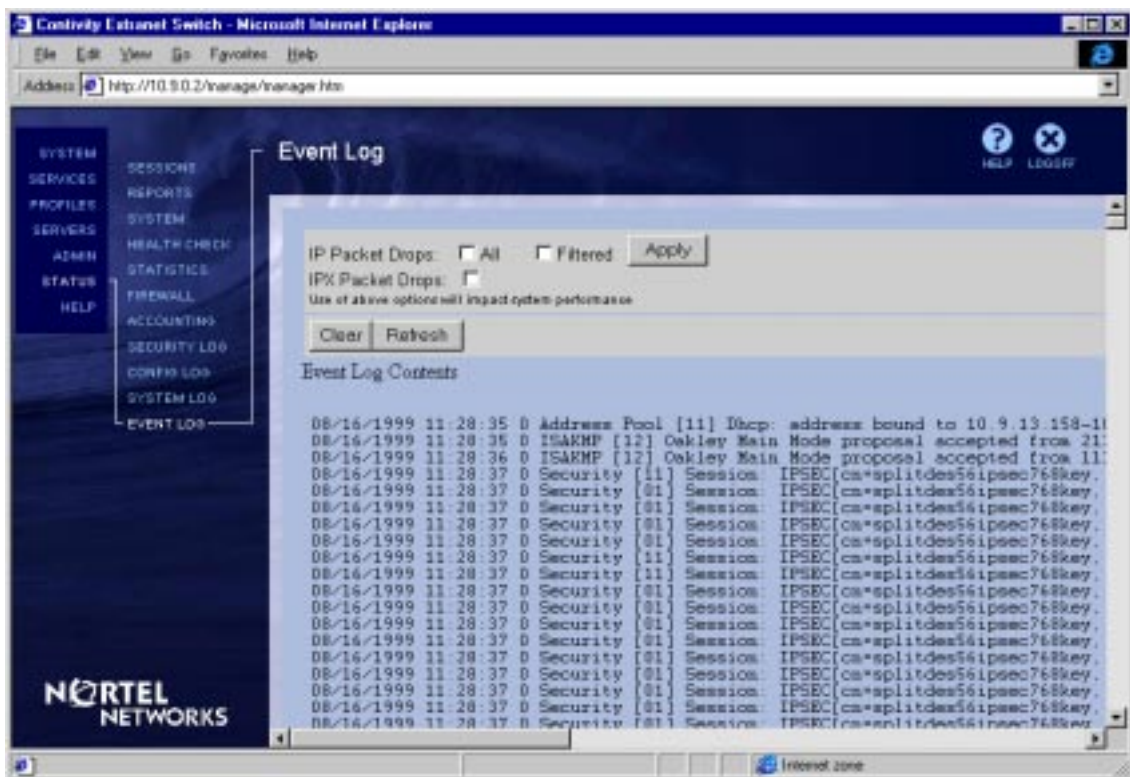
Event Log

The Event Log is a detailed recording of all events that take place on the system. These entries are not necessarily written to disk, as with the System Log. The Event Log retains all system activity in-memory but only the significant entries are saved in the System Log (on disk).

The Event Log includes information on tunneling, security, backups, debugging, hardware, security, daemon processes, software drivers, interface card driver events, and so forth.

As the Event Log adds in-memory information, its oldest entries are overwritten. The Event Log retains the latest 2000 entries, and discards old entries when it is refreshed.

Figure 156 Event Log



IP/IPX Packet Drops

This option logs an IP/IPX dropped packet header (source and destination address). Packets can be dropped due to filtering, corruption, and so forth. Refer to "The following table provides descriptions of active sessions." for additional information.

All Packets

This option logs the contents of all packets.

Filtered Packets

This option logs the contents of filtered packets.

Clear

Click to Clear the entire log. Only Administrators can clear the log.

Refresh

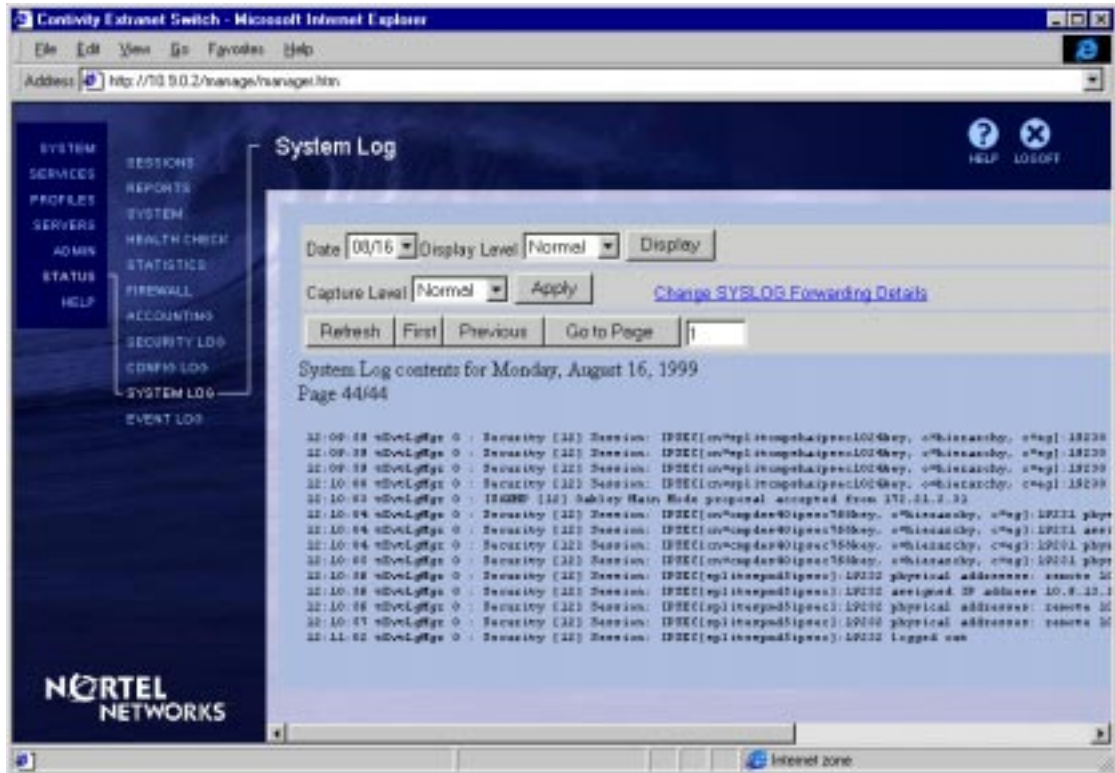
Click to display new log entries.

System Log

The System Log contains all System events that are considered significant enough to be written to disk, including those displayed in the Configuration and Security Logs. Examples of events that would appear in the System Log include:

- LDAP activity
- Configuration activity
- Server authentication and authorization requests

Figure 157 System Log



System Log Contents for *Date*

This is the date (day/month/year) of the log file that is currently being displayed. When you change the Date field, then click Display, the new date's log file is displayed and the System Log Contents for *date* field changes to reflect the new request.

Capture Level

The Capture Level option allows you to filter between saving to disk all events including Debug events, and saving Normal and Urgent events only.



Note: Capturing All Events adds a small amount of system overhead and similarly takes a minor toll on performance. Therefore, you should probably capture Debug events at the request of Nortel Networks personnel only.

Normal

These are the events that are normally of typical interest to you.

Urgent

These events would be of critical interest to you. They could represent a severe security or access problem; or even something that might have happened accidentally but if it recurred would be cause for concern.

All

These events allow Nortel Networks Customer Support personnel to learn additional factors that might be contributing to a problem.

Security Log

The Security Log records *all* activity about System or User security. The Security Log lists all security events, both failures and successes. The events can include:

- Authentication and authorization events
- Tunnel or administration requests
- Encryption, authentication, or compression
- Hours of access
- Number of session violations
- Communications with servers

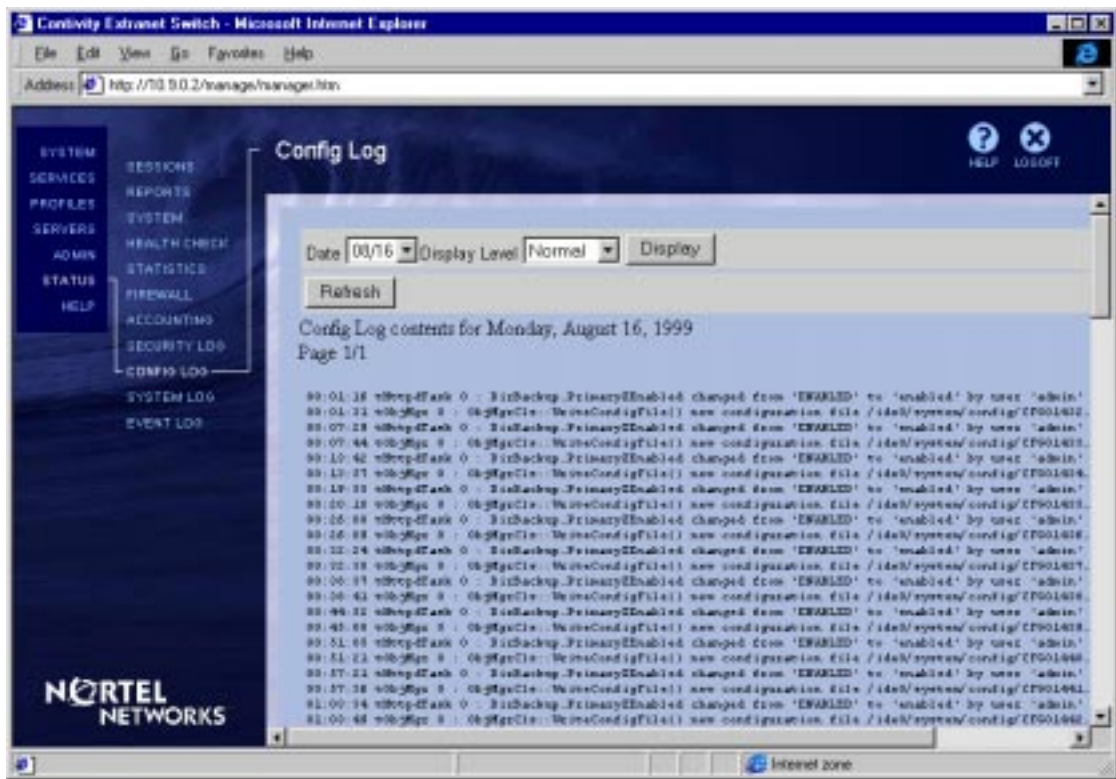
- ## Security Log

Configuration Log

The Configuration Log records all configuration changes. For example, it tracks adding, modifying, or deleting configuration parameters:

- Group or user profiles
- LAN or WAN interfaces
- Filters
- System access hours
- Shutdown or startup policies
- File maintenance or backup policies

Figure 159 Configuration Log



Index

A

- accessible networks 338
- ACK bit filter 308
- active sessions
 - details 432
 - viewing 427
- add group 254
 - branch office 330
- add remote network 343
- address control field compression 90
- address filters 306, 309
- address pool
 - end address 327
 - external NAT 327
 - internal 458
 - NAT 327
 - NATinternal 326
 - start address 326
- admin rights 293
- administrator
 - privileges user configuration 293
 - settings 374
- admission control 249
- alert, health check 448
- Allow All
 - branch office 331
 - enabling 108
 - enabling clients 107
- alternate RADIUS server 348
- associated group authorization 135
- asterisk logging 469

- authentication 135, 267
 - branch office 339
 - methods 280
- automatic backup 378
- available rules 237, 298
- AXENT 131, 135, 268, 347

B

- backup
 - configuration 388
 - restore 352
- bandwidth management 248
- bandwidth rate 249
- base distinguished name 355
- base group 251
- bind
 - distinguished name 357
 - password 357
- BIOS 445
- brackets numbers, logging 469
- branch office
 - authentication 339
 - define connection 334
 - edit connection 336
 - edit group 330
 - routing 333

C

- cable modems 281
- call admission priority 259
- capture level system log 473

- certificates
 - branch office 339
 - CRL retrieval 128
 - details 114
 - fingerprint 114
 - owner 115
- CHAP 87, 89, 135, 138, 139, 143, 277, 279, 281, 347
- children, base group 251
- client fail-over 273
- client policy 275, 344
- client-specified address 281
- comma delimited 437
- common fields
 - filtering 309
 - logging 467
- common name 110
- components, health check 448
- compression 90, 91, 273, 279, 281
- configuration
 - boot 424
 - file 458
 - initial 256
 - log 466, 475
 - user rights 294
- Configure IP 331
- connection name, branch office 335
- Contivity Firewall
 - logging 156
- Contivity Stateful Firewall 153
- control tunnels 336
- counters, LAN interface statistics 71, 77
- country 111
- CRL 128
 - update frequency 117
- CSU/DSU 83
- current configuration 256
- current networks 320

- current subnetworks 322
- current time 101

D

- date and time 101
- debug events 165, 468
- debug system log 473
- default group
 - client authentication 108
 - RADIUS 347
- default nearest server 94
- default rule, filters 305
- deny packet filter 306
- DES encryption 133, 269
- Diffie-Hellman 270
- DiffServ 247
- direction
 - inbound filter 306
 - outbound filter 306
- diskette drive 446
- DNS 55, 57, 277, 279
 - primary 57, 282
 - secondary 58, 282
 - tertiary 58
- Domain Name System 57
- DSCP Value 241
- Dynamic Host Configuration Protocol 361

E

- echo
 - fault threshold 91
 - interval 91
- edit
 - branch office connection 336
- edit filter 298
- egress queueing mode 247
- encryption 131, 269

end address, NAT 327
Ethernet interface 60, 95
event log 466, 470
external
 DHCP 362, 363
 dynamic host configuration protocol 361
 LDAP 352
 LDAP server 353
external address
 endpoint device 327
 NAT 327

F

factory default 386
 configuration 388
fail-over 136
file system 456
 maintenance 396, 398
 details 399
filter rules 305
filters 262, 295
 branch office 338
 common fields 309
 copy 296
 delete 296
 edit 296, 298
 edit current 296
 storing 296
fingerprint
 certificate 109, 114, 116
Firewall
 Contivity Stateful Firewall 153
firewall type 162
forwarding priority 259
FQDN user configuration 291
FTP 128, 300, 301
 software version 393
full distinguished name
 branch office 293, 341

full reformat recovery 386
fully qualified domain name
 authentication server 347, 352, 355
 LDAP server 356
 user configuration 291

G

graphs 435
group
 branch office name 330
 edit 256
 ID 268
 name 255
 password 268
 password authentication 135
 user configuration 284, 288
groups 251
 inherited 252

H

hard drive
 disk space 445
 reformatting 389
hardware
 encryption accelerator 96
 health check 446
health check 448
historical event logging 466
hours of access
 editing 318
 setting 317
HTTP 127, 128

I

ICMP
 filter 240, 307
 statistics 455
ide0 root disk drive 352
idle timeout 261, 376

IKE
 encryption 270
 Internet Key Exchange 270

inheritance
 configuration 252
 group 254

initial configuration 256

interface
 characteristics 454
 classifiers 235
 debug 92
 description 60
 QoS Statistics 247

Interface shaping 244

internal
 address pool 364
 LDAP 351
 NAT address pool 326

Internet domain 57

Internet Security Association Key Management
 Protocol 129, 264

Internetwork Packet Exchange 92

interval
 session update 359, 360
 SNMP check 406

IP address
 branch office 337
 changing system 55
 currently assigned 61
 remote 82
 user configuration 288

IP filter 307

IP packets 240

IP statistics 456

IPCP 80, 89
 settings 91

IPSec 129, 264
 transport mode connections 277
 user configuration 291

IPX 92

IPX configuration 93

ISAKMP 129, 264

ISP 87, 281

J

Japanese GUI 377

K

Kanji GUI 377

L

L2F 142
 NAS edit 145
 user configuration 291

L2TP 138
 NAS edit 140
 user configuration 277, 291

L2TP/IPSec 277

LAC L2TP access concentrator 141

LAN
 card 60, 62, 95
 counters 457
 interface statistics 71

last name search 285

LCP 89, 90

LDAP
 attribute search 285
 authentication 135
 directory backup 352
 master server 356
 restore database file 353
 server port number 117
 user configuration 286

LDIF 353
 legacy forwarding priority 247
 load balancing 136
 locality 111
 log file

- life time 121
- Log File Configuration 121
- log off 431
- logging 156
 - common field descriptions 467
 - task name 469
 - task type 469
- logins, disabling 423

M

- MAC address 445
- management
 - IP address 56
 - protocols 127
- master LDAP server 356
- MBONE 240, 307
- MD5 133, 270
- memory 455
 - system 445
- Message Digest 5 133, 270
- message logging 469
- MF Classifiers 236
- MIB 401
- Microsoft Point-to-Point Compression 281
- MPPC 281
- MS-CHAP 135, 138, 139, 277, 280, 347
- multi-field classifiers 236

N

- NAS 142, 144, 277, 278
 - passwords 146
 - UIDs 144
- network access server 277
- Network Address Translation (NAT) 326
- networks
 - branch office 320
 - split tunneling 320

- new rule 302
- new subnetworks 322
- non-tunneled traffic 244
- normal events
 - logging 165, 468

O

- OmniGuard/Defender 135, 268
- organizational unit 110
- OSPF 177
 - configuration 178
 - known areas 180
 - overview 177
- override default configurations 256
- over-subscription ratio 244

P

- packet filtering 262
 - permit 306
- PAP 88, 139, 143, 277, 279, 281
- parent group 255
- per-hop behavior 247
- PKCS #10
 - certificate request 111
- PKCS #7
 - base-64 certificate 112
 - importing encoded certificate 109
- Point-to-Point Tunneling Protocol 276
- pooled translation type 326
- port translation type 326
- ports
 - destination filter 241, 307
 - LDAP 356
 - RADIUS accounting 360
 - RADIUS authentication 349
 - source filter 241, 307
 - SSL 357
- PPP 80

- advanced settings 83
- authentication settings 83
- PPTP 137, 276, 291
- pre-shared key 339
- primary
 - administrator 375
 - administrator password 376
 - RADIUS server 348
 - Windows Internet Naming Service (WINS) 282
- processors 445
- protocol
 - field compression 91
 - filters 240, 307, 312
- proxy ARP 122
- public data network 60
- public key sizes 111
- public network address, IPX 93

Q

- QoS
 - for groups 235
 - interfaces 242
 - statistics 247
- queueing mode 247
- quick reformat 386

R

- RADIUS 128
 - authentication 135, 346
 - L2F 143
 - servers 348
 - user configuration 286
- RC4-128 280
- RC4-40 280
- recovery 384
- recovery diskette 386
- rekey data count 274
- rekey timeout 274

- remote identity 339
- remote IP address 82
- reports 436
- reset button 391
- restore LDAP database 352
- retrieve latest software 393
- RIP 188
- routing policy 223
- routing table 455
- RSVP 262, 263
- rule definition filters 303

S

- safe mode 119
- screen saver password 272
- search for users 285
- secret for RADIUS servers 350
- secure hash algorithm 100, 133, 269
- SecurID 268, 347
- security
 - log 466, 473
- Security Dynamics SecurID 135
- Security Dynamics SecurID 131, 268, 347
- security statistics 457
- serial number 389, 445
- server
 - LDAP 354
 - secret
 - RADIUS accounting 350, 360
 - status
 - RADIUS accounting 350, 360
- server certificate 113
 - branch office 341
- session details 432
- SHA 100, 133, 269
- shutdown
 - after power off 424

- now 424
- time 423
- slapd 457
- slave 1 LDAP server 356
- slave 2 LDAP server 356
- SNMP 128, 300
 - trap hosts 403, 404
 - trap interval 406
 - version 1 traps 401
- software
 - build date 445
 - FTP 392
 - health check 446
 - version 390, 444
 - apply 393
 - new 386
- split tunneling 265
- SSL
 - port 636 357
 - port number 117
- state/province 111
- static
 - addresses allowed 261
 - IP address 288
 - translation type 326
- static routes
 - add private route 171
 - add route 174
 - default routes 168
 - edit existing 173
 - enable 168
 - overview 167
 - show branch office routes 176
 - through physical interface 172
- statistics 61, 71, 77
 - display 453
 - hardware encryption accelerator 101
- status for health check 448
- subject distinguished name 108
- subnet mask 62

- system
 - configure identity 55
 - log 466, 471
 - services display 125
 - shutdown 421
 - status 443
- system forwarding 122

T

- T-1 83
- TCP
 - connection 308
 - filter 308
 - filter 240, 307
 - statistics 455
- Telnet 128
- third party clients
 - configuring 266
 - supported 266
- time stamp for logging 469
- token bucket 263
- traffic conditioning 246
- translation types 326
- troubleshooting
 - LAN interface statistics 71
 - WAN interface statistics 77
- trusted CA certificate 107, 113
- tunnel to tunnel settings 122
- tunnel types 125, 126, 127

U

- UDP
 - filter 240, 307
 - statistics 455
- up time system 444
- update frequency 117
- upgrades 391
- urgent events

logging 165, 468
user
 add 285
 configuring rights 294
 ID search 285
 management configuration 283
 name 288
User Bandwidth Policy 263
 Committed Rate 263
 Excess Action 263
 Excess Rate 263
X.500 distinguished name 109
xDSL 281
XNS 92

V

valid issuer certificate authority
 branch office 340
Van Jacobson compression 91
version for software 454
VJ
 compression 91
 identification compression 92
 max slots 92
 negotiation 91

W

WAN interfaces
 advanced settings 89
 currently installed 74
 settings 80
 statistics 77
 status 457
warning, health check 448
wildcard 312
WINS 277, 279, 282
 primary 282
 secondary 283
write access, LDAP server 356

X

X.500 directory search base 117